WatchGuard XCS

Extensible Content Security 9.1 Update 2 User Guide

WatchGuardXCS
170,370,570,770,770R,970,1170

About this User Guide

The *WatchGuard XCS User Guide* is updated with each major product release. For minor product releases, only the *WatchGuard XCS Help* system is updated.

Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

Guide revised: 2/7/2011

Copyright, Trademark, and Patent Information

> ***Note*** *This product is for indoor use only.*

About WatchGuard

WatchGuard offers affordable, all-in-one network and content security solutions that provide defense-in-depth and help meet regulatory compliance requirements. The WatchGuard XTM line combines firewall, VPN, GAV, IPS, spam blocking and URL filtering to protect your network from spam, viruses, malware, and intrusions. The new XCS line offers email and web content security combined with data loss prevention. WatchGuard extensible solutions scale to offer right-sized security ranging from small businesses to enterprises with 10,000+ employees. WatchGuard builds simple, reliable, and robust security appliances featuring fast implementation and comprehensive management and reporting tools. Enterprises throughout the world rely on our signature red boxes to maximize security without sacrificing efficiency and productivity.

Table of Contents

1 WatchGuard XCS Overview

About the WatchGuard XCS

The WatchGuard XCS is the industry's first consolidated messaging security platform delivering integrated protection, control, and management for email and web content.

Firewall-level Network and System Security

The WatchGuard XCS delivers the most complete security available for messaging systems. The system runs on a customized and hardened Unix operating system, and does not allow uncontrolled access to the system. There is no command line access and the WatchGuard XCS runs as a closed system, preventing accidental or deliberate misconfiguration by administrators, which is a common cause of security vulnerabilities.

Message Delivery Security

The WatchGuard XCS content security features provide instant-on data loss prevention, encryption and content filtering with integrated threat prevention for viruses, spam, spyware, phishing, and malware attacks, all in a secured appliance. In addition, the WatchGuard XCS protects outbound content against unintentional or malicious data loss, privacy discrepancies and non-compliance with regulations and company policies.

The WatchGuard XCS utilizes a sophisticated message delivery system with several security features and benefits to make sure that the identifying information about your company's messaging infrastructure remains private.

For a company with multiple domain names, the system can accept, process, and deliver mail to private email servers. For a company with multiple private email servers, the system can route mail based on the domain or subdomain to separate groups of email users.

Web Security

The WatchGuard XCS incorporates a Web Proxy that allows the system to proxy web traffic and control access to external web sites. The system can scan web traffic using a subset of the same scanners that examine email messages to inspect the content of web traffic and downloaded files. Policy features apply specific HTTP access policies to different users, groups, IP addresses, and domains, and you can customize notifications for blocked connections or files and send them to the administrator and recipient.

The Web Traffic Accelerator solution provides critical Web traffic enhancements, for example, disk caching and streaming media support, that reduce bandwidth consumption, server loads, and latency to improve network performance.

Web Reputation allows you to block web site domains that have a bad reputation for hosting viruses and malware.

Content Controls

The WatchGuard XCS implements attachment control, content scanning, and content filtering based on pattern and text matching. The content controls prevent these issues:

- Breaches of confidentiality
- Legal liability from offensive content
- Personal abuse of company resources
- Breaches of compliance policies

Attachment controls are based on these characteristics:

- **File Extension Suffix** – The suffix of the file is checked to determine the attachment type, for example, .exe, or .jpg.
- **MIME Content Type** – Use MIME (Multipurpose Internet Mail Extensions) to identify the actual content type of the message.
- **Content Analysis** – The file is carefully scanned to look for characteristics that can correctly identify the file or MIME type. This analysis makes sure that the attachment controls are not circumvented by simply renaming a file.
- **Content Scanning** – Attachments, for example, Adobe® PDFs or Microsoft® Word documents, are analyzed for words or phrases that match a pattern filter or compliance dictionary.

Virus and Spyware Scanning

The WatchGuard XCS features a virus scanning engine based on Kaspersky® Anti-Virus. You can scan email messages and web requests in both inbound and outbound directions for viruses and spyware. The high performance scanning provides a vital layer of protection against viruses for your entire organization. Automatic pattern file updates make sure that the system can detect the latest viruses and spyware.

McAfee® Anti-Virus is also available as an add-on subscription for customers who want to enable multi-layered Anti-Virus protection.

Outbreak Control

The Outbreak Control feature provides customers with zero-day protection against early virus outbreaks. For most virus attacks, it can be several hours from the moment the virus is released to the time a pattern file is available to protect against the virus. During this period, mail recipients are vulnerable to potential threats. The Outbreak Control feature detects and takes action against early virus outbreaks to contain the virus threat.

Malformed Message Protection

Similar to malformed data packets used to subvert networks, malformed messages allow viruses and other attacks to avoid detection, crash systems, and lock up mail servers. The WatchGuard XCS makes sure that only correctly formatted messages are allowed into your mail systems. Message integrity checking protects your mail servers and clients and improves the effectiveness of existing virus scanning implementations.

Intercept Anti-Spam

The WatchGuard XCS provides a complete set of Anti-Spam features specifically designed to protect against the full spectrum of current and evolving spam threats. Intercept combines the results of several Anti-Spam components to provide a better informed decision on whether a message is spam or legitimate, mail while minimizing false positives. These features include:

- **Spam Words** – Filters messages based on a dictionary of typical spam words and phrases that are matched against a message.
- **Mail Anomalies** – Checks various aspects of the incoming message for issues, for example, unauthorized SMTP pipelining, missing headers, and mismatched identification fields.
- **DNS Block List (DNSBL)** – Detects spam using domain-based lists of hosts with a bad reputation. Messages can also be rejected immediately regardless of the results of other Anti-Spam processing if the client is listed on a DNSBL. A configurable threshold allows you to specify how many DNSBLs must trigger to consider the sender as unreliable.
- **URL Block List** – Examines the URLs in a message and queries a SURBL (Spam URI Real-time Block Lists) server to determine if this URL has been used previously in spam messages.
- **Reputation Enabled Defense (RED)** – The Reputation Enabled Defense feature helps to identify spam by reporting a collection of metrics about the sender of a message. This includes their overall reputation, whether the sender is a dial-up, and whether the sender appears to be virus-infected, based on information collected from installed customer products and global DNS Block Lists. This information is used by Intercept to reject the message, or contributes to the overall Anti-Spam score for the message. Reputation Whitelists allow you to train on messages from known legitimate sources based on their reputation.
- **Token Analysis** – Detects spam based on advanced content analysis using databases of known spam and valid mail. This feature is also specially engineered to effectively detect image spam.
- **Backscatter Detection** – Detects spam based on signature verification of the Envelope Sender to prevent spam bounce emails to forged sender addresses.
- **Sender Policy Framework (SPF)** – Performs a check of a sending host's SPF DNS records to identify the source of a message.
- **DomainKeys Authentication** – Performs a check of a sending host's DomainKeys DNS records to identify the source of a message.

- **Brightmail** – Symantec Brightmail™ Anti-Spam is an add-on subscription for customers who want to enable multi-layered Anti-Spam engines. Brightmail integrates into the overall Intercept spam score, or you can run Brightmail independently.

Reputation Enabled Defense (RED)

The Reputation Enabled Defense (RED) feature helps to identify spam by reporting behavioral information about the sender of a message. This includes their overall reputation, whether the sender is a dial-up, and whether the sender appears to be virus-infected or sends large amounts of spam messages, based on information collected from installed customer products and global DNS Block Lists. Domain and Sender Reputation increases the effectiveness of RED by examining not only the IP reputation of a sender, but also the domain name and envelope sender information from that IP address. This information is used by the WatchGuard XCS to reject the message immediately or contribute to the Intercept score if a message is detected from a source with a bad reputation.

If you enable Reputation checks, the WatchGuard XCS queries the statistics on the RED domain service for the sender IP address of each message received, excluding those addresses from trusted and known networks. Web Reputation is also available to block access to web sites that have a bad reputation for hosting viruses and malware.

Using the information returned from RED, the WatchGuard XCS makes a decision about whether a message is spam or legitimate mail. A reputation closer to 0 indicates the sender is extremely reliable and rarely sends spam or viruses. A reputation closer to 100 indicates the sender is extremely unreliable and often sends spam or viruses. An IP address with no previous information from any source is assigned an initial neutral value of 50.

Trusted and Blocked Senders Lists

End users can create their own personal Trusted and Blocked Senders Lists based on a sender's email address. The Trusted email addresses are exempt from Anti-Spam scanning, allowing users to trust legitimate senders, while email addresses on the Blocked Senders List are prevented from sending mail to that user through this WatchGuard XCS.

Spam Quarantine

The Spam Quarantine redirects spam mail into a local storage area for each individual user. Users can connect to the WatchGuard XCS directly or through a summary email to view and manage their own quarantined spam. Users can delete messages, or move them to the user's local mail folders. You can send automatic notifications to end users notifying them of the existence of messages in their personal quarantine area.

The integrated User Spam Quarantine feature on the WatchGuard XCS supports a single end-user notification domain. End users can have multiple email addresses, but the notification system supports only a single, primary email domain.

For large enterprises, a dedicated Quarantine Management Server (QMS) is available that supports up to 100,000 quarantine users from multiple domains, and supports clustering for redundancy.

Microsoft Outlook Add-in

The WatchGuard XCS Outlook Add-in places special **Spam** and **Not Spam** buttons on your Microsoft Outlook client toolbar. This tool allows you to report any spam messages that bypassed the spam filters and were delivered to their inbox, and also report false positives where legitimate messages were classified as spam.

Threat Prevention

Threat Prevention allows organizations to detect and block real-time incoming threats. You can monitor and record threat types to track client IP behavior and reputation. By examining message flow patterns, the WatchGuard XCS detects whether a sending host is behaving maliciously by sending out viruses, spam, or attempting denial-of-service (DoS) attacks. By instantly recognizing these types of patterns, Threat Prevention presents an effective solution against immediate, real-time attacks. The Threat Prevention feature blocks or throttles inbound connections before the content is processed to lessen the impact of a large number of inbound messages.

Secure WebMail

Secure WebMail provides remote access support to internal mail servers. With Secure WebMail, users can access their mailboxes with email web clients, for example, Outlook® Web Access, Lotus iNotes, or the WatchGuard XCS web mail client. The WatchGuard XCS addresses the security issues that prevent deployment of web mail services with these features:

- Strong authentication (includes integration with Active Directory)
- Encrypted sessions
- Advanced session control to prevent information leaks on workstations

Authentication

The WatchGuard XCS supports these authentication methods for administrators, WebMail users, Trusted/Blocked Senders List, and Spam Quarantine features:

- User ID and Password
- LDAP
- RADIUS
- RSA SecurID® tokens
- SafeWord and CRYPTOCard tokens

Integrated and External Message Encryption

The WatchGuard XCS provides an integrated message encryption option and also includes integration with external encryption servers to provide email encryption and decryption functionality. Email encryption allows users to encrypt individual messages by the integrated encryption service or through a separate encryption server before the messages are delivered to their destination by the WatchGuard XCS.

Incoming encrypted messages are sent to the encryption server to be decrypted before the WatchGuard XCS accepts the message and delivers it to the intended recipient. This integration allows organizations to make sure that encrypted messages are still processed for security issues, for example, viruses, malformed mail, and content filtering and scanning.

Mail Delivery Encryption

You can encrypt all messages delivered to and from the WatchGuard XCS with TLS (Transport Layer Security). This includes connections to remote systems, local internal mail systems, or internal mail clients. Encrypted messages are delivered to local and remote destinations with complete confidentiality.

Use TLS encryption for:

- Secure mail delivery on the Internet to prevent anyone from viewing email messages while in transit
- Secure mail delivery across a LAN to prevent malicious users from viewing email messages other than their own
- Create policies for secure mail delivery to branch offices, remote users and business partners
- Supports TLS/SSL encryption for all user and administrative sessions.
- Use TLS/SSL to encrypt SMTP sessions that prevents eavesdropping and interception

Policies

Policy-based controls allow settings for the WatchGuard XCS security features, for example, Annotations, Anti-Spam, Anti-Virus, and Attachment Control, to be customized and applied based on the group membership, domain membership, IP address, or email address of the recipient.

You can import user group membership information from an LDAP-based directory, and then create policies to apply customized settings to these groups. For example, you can set up an Attachment Control Policy to allow your Development group to accept and send executable files (.exe). You can then customize your Attachment Control settings for all your other departments to block this file type and prevent the spread of viruses among the general users.

In addition, you can add an effective time period to apply to any policy, based on the current time and day of the week.

Directory Services

The WatchGuard XCS integrates with LDAP (Lightweight Directory Access Protocol) directory services, for example, Active Directory, OpenLDAP, and iPlanet, to utilize these features:

- **LDAP lookup prior to internal delivery** – The WatchGuard XCS can check for the existence of an internal user through LDAP before delivering a message. This feature allows you to reject mail to unknown addresses in relay domains, reducing the number of attempted deliveries of spam messages for non-existent local addresses. This check is performed directly to an LDAP server or to a cached directory stored locally on the system.
- **Group/User Imports** – An LDAP lookup determines the group membership of a user when applying policy-based controls. You can also import LDAP users and mirror their accounts on the WatchGuard XCS to use for features like the Spam Quarantine.

- **Authentication** – You can use LDAP for authenticating Web Proxy access, IMAP access, user mailbox, and WebMail logins.
- **SMTP Relay Authentication** – You can use LDAP for authenticating clients for SMTP Relay.
- **Mail Routing** – You can use LDAP to lookup mail route information for a domain to deliver mail to its destination server.

System Management

The WatchGuard XCS provides a complete range of monitoring and diagnostics tools to monitor the system and troubleshoot mail delivery issues. Admin sessions are encrypted for additional security, while comprehensive logs record all message and admin activity.

- **Web Browser-based management** – The web browser management interface displays a live view of system activity and traffic flows. You can configure the management interface to display information for a single system or many systems in a local cluster or in a centralized management configuration.
- **Dashboard** – The WatchGuard XCS system Dashboard provides administrators with a brief statistical and graphical summary of current inbound and outbound email and web activity. This allows rapid assessment of the current status of the WatchGuard XCS.
- **Enterprise integration with SNMP** – With SNMP (Simple Network Management Protocol), the system can generate both information and traps to be used by SNMP monitoring tools. This extends your view of the WatchGuard XCS and provides you with notification of significant system events, for example, excessive traffic flows and system failures.
- **Alarms** – The system generates system alarms that automatically notify you through email and Dashboard alerts of a system condition that requires attention.
- **Archiving** – Archiving support allows organizations to define additional mail handling controls for inbound and outbound mail. These features are especially important for organizations that must archive certain types of mail for regulatory compliance or for corporate security policies.

Clustering

The WatchGuard XCS clustering feature provides a highly scalable, redundant messaging security infrastructure that enables two or more XCS devices to act as a single logical unit for processing messages while providing redundancy and high availability benefits. There is no theoretical limit to the size of the cluster, and you can easily add devices to the cluster to increase processing and high-availability capabilities. Clustering makes sure that the flow of traffic is not interrupted due to individual system failures. You can manage a cluster from any single device in the cluster without the need for a separate management console, and all devices in the cluster can process messages. Any configuration changes, for example, Anti-Spam and Policies, are propagated to all devices in the cluster.

Reports

WatchGuard XCS reports provide a comprehensive range of detailed reporting information that can be generated in PDF (Adobe Portable Document Format), CSV, and HTML format on demand and at scheduled times. The reports are derived from information written to the systems and message logs that are stored in the message database. Up to a month's reporting data can be stored and viewed online depending on message loads for a particular environment. Reports are stored on the system for online viewing, and can also be emailed automatically to the administrator.

In clustered environments, reports aggregate information for the entire cluster. System and resource reports display information for each system in the cluster.

For organizations that support multiple domains, you can add per domain information to the reports providing you with statistics for each hosted domain. You can also enable Hosted domain reports that create separate reports for a specific domain and can be emailed to the administrators of each hosted domain.

Security Connection

The Security Connection provides an automated software update service that polls WatchGuard's support servers for new updates, security alerts, and Anti-Spam database updates. You can be notified when new software updates are available for installation.

Internationalization

The WatchGuard XCS supports internationalization for annotations, notification messages, and message database views. For example, if a message is sent to someone who is on vacation and the message used character set ISO-2022-JP (Japanese), the vacation notification sent back is in the same character set. You can view the message history database with international character sets.

The WatchGuard XCS also supports the ISO-8859-1 (Western European Languages) based character set for dictionary-based content filtering with the Objectionable Content Filter.

WatchGuard XCS Deployments

The WatchGuard XCS is designed to be situated between internal email servers and clients, and external servers on the Internet so that there are no direct connections between external and internal systems.

The WatchGuard XCS is installed in one of these locations:

- On the DMZ (Demilitarized Zone) of a network firewall
- In parallel with a network firewall
- Behind the existing firewall on the internal network

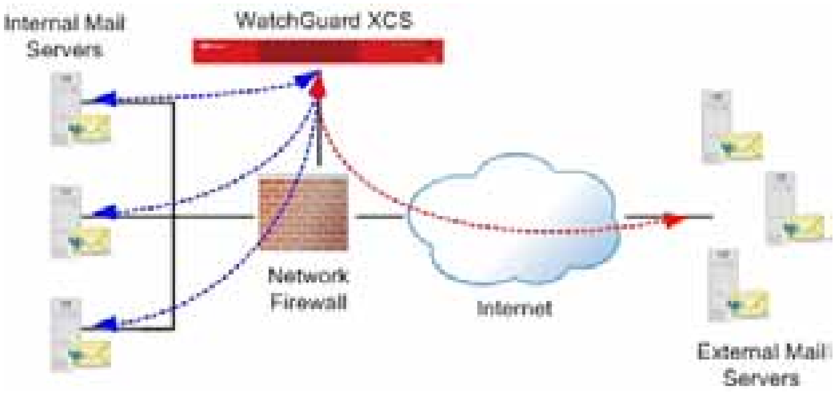
Messaging traffic is redirected from either the external interface of the network firewall or from the external router to the WatchGuard XCS. When the WatchGuard XCS accepts and processes a message, the device initiates a connection to the internal mail servers to deliver the messages.

WatchGuard XCS on the DMZ of a Network Firewall

The most common deployment strategy for the WatchGuard XCS is to be situated on the DMZ of a network firewall. This type of deployment prevents any direct connections from the Internet to the internal mail servers, and makes sure the WatchGuard XCS is located on a secure network behind the firewall.

This deployment uses a single network interface connected to the DMZ network of the network firewall.

The Installation Wizard helps you install the WatchGuard XCS in this deployment configuration.

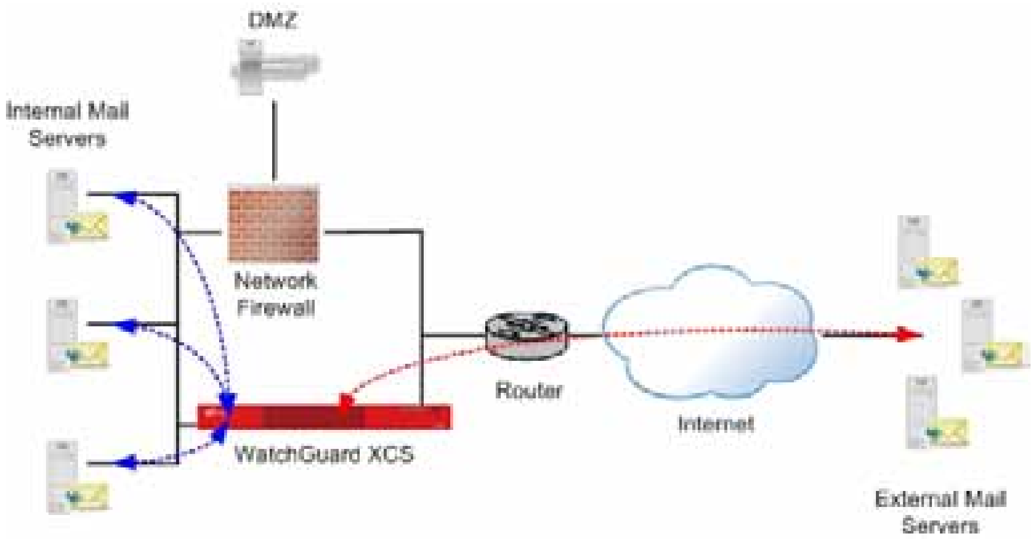


WatchGuard XCS in Parallel with a Network Firewall

You can deploy the WatchGuard XCS in parallel with an existing network firewall. The device's firewall security architecture eliminates the risk associated with deploying an appliance on the perimeter of a network.

This parallel deployment eliminates any messaging traffic on the network firewall and decreases its overall processing load.

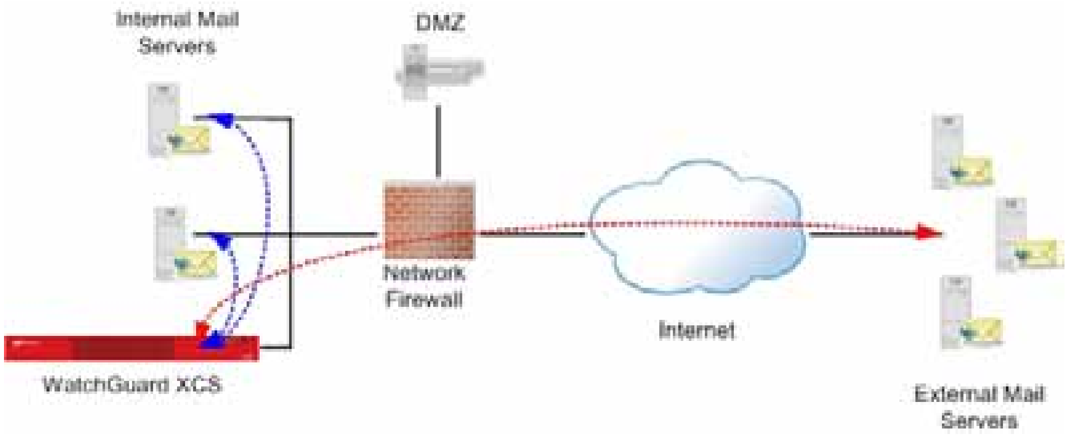
A second network interface must be configured to connect to the Internet-facing network.



WatchGuard XCS on the Internal Network

The WatchGuard XCS can also be deployed on the internal network. Although this configuration allows a direct connection from the Internet to the internal network, it is a legitimate configuration when required by existing network resources.

This deployment uses a single network interface connected to the DMZ network of the network firewall.



How Messages are Processed

These sections describe the sequence in which the WatchGuard XCS security features are applied to any inbound and outbound messages and how these settings affect their delivery.

Trusted Messages

The system only processes messages through the spam filters when a message originates from an untrusted source. Messages from trusted sources bypass the spam controls. By default, messages that arrive on a particular network interface from the same subnet are trusted.

There are two ways to control how message sources are identified and trusted:

- The network interface the message arrives on
- A specified IP address (or address block), or server or domain name

See *Trusted and Untrusted Mail Sources* for information on how the WatchGuard XCS determines the source of a message.

Inbound and Outbound Scanning

For features that scan both inbound and outbound messages, these rules apply:

- Mail from trusted source to local recipient – Inbound
- Mail from trusted source to non-local recipient – Outbound
- Mail from untrusted source to local recipient – Inbound
- Mail from untrusted source to non-local recipient – Inbound

SMTP Connection

An SMTP connection request is issued from a sending server. The WatchGuard XCS accepts the connection request unless one of these checks (if enabled) triggers:

- **Reject on Threat Prevention** – Rejects mail when the client is rejected by the Threat Prevention feature.

- **Reject on missing addresses** – Rejects mail when no recipients in the To: field, or no senders in the From: field are specified in the message headers.
- **Maximum number of recipients** – Rejects mail if the number of recipients exceeds the specified maximum (default is 1000).
- **Maximum message size** – Rejects mail if the message size exceeds the maximum.
- **Reject on unauthorized SMTP pipelining** – Rejects mail when the client sends SMTP commands ahead of time without knowing that the mail server actually supports SMTP command pipelining. This stops messages from bulk mail software that improperly use SMTP command pipelining to speed up deliveries.
- **Reject on expired license** – Rejects mail if the system license is expired.
- **Specific Access Pattern and Pattern Based Message Filter (Reject)** – Rejects mail based on Specific Access Patterns and Pattern Filters for the HELO, Envelope-To, Envelope-From, and Client IP fields.
- **Connection Rules Reject** – Rejects mail based on any configured Connection Rules.
- **Reject on DNS Blocklist** – Rejects mail if the sender is on a DNSBL and the system is set to reject on DNSBL.
- **Reject on Reputation Enabled Defense (Reputation, Infected, Dial-up)** – Rejects mail based on statistics provided by the Reputation Enabled Defense service.
- At this point, trusted or local networks skip any further Reject checks.
- **Reject on Backscatter Detection** – Rejects mail when the message fails the Backscatter signature verification.
- **Reject on unknown sender domain** – Rejects mail when the sender mail address has no DNS A or MX record.
- **Reject on missing reverse DNS** – Rejects mail from hosts if the host IP address has no PTR (address to name) record in DNS, or when the PTR record does not have a matching A (name to address) record. This setting is rarely used because many servers on the Internet do not have valid reverse DNS records, and enabling this feature can result in rejecting mail from legitimate sources.
- **Reject on missing sender MX** – Rejects mail when the sender’s mail address is missing a DNS MX record.
- **Reject on non-FQDN sender** – Rejects mail when the address in the client MAIL FROM command is not in the form of a fully-qualified domain name (FQDN).
- **Reject on Unknown Recipient** – Rejects mail if the specified recipient does not exist. The WatchGuard XCS performs an LDAP lookup on the recipient’s address to make sure they exist before it delivers the message.

Virus and Spyware Checking

Messages are scanned for viruses and spyware. If there is a virus or spyware program detected, the system can perform a variety of actions, for example, reject or quarantine.

Malformed Message Checking

The WatchGuard XCS analyzes each message with extensive integrity checks. Malformed messages (which could be hidden viruses or attempts at a denial-of-service attack) can be quarantined, rejected, or discarded if they cannot be processed.

Attachment Size Limits

The size of all attachments are checked to make sure they do not exceed the attachment size limit threshold.

Attachment Control

Message attachments are scanned for blocked content. If there is a problem, the system can perform a variety of actions, for example, sending the message to the quarantine area. Attachments can also be stripped, and then the message continues other security processing.

Outbreak Control

Messages are scanned by Outbreak Control to look for virus-like behavior. These messages can be quarantined until updated anti-virus pattern files are available to rescan them.

If Malformed Mail or the Attachment Control feature rejects or discards a message, the Outbreak Control feature takes precedence, and the Malformed or Attachment Control action is applied when the message is released by Outbreak Control.

OCF (Objectionable Content Filter)

Messages are scanned for objectionable content with a pre-defined dictionary of words. A configurable action is performed on the message if any content matches words or phrases in the dictionary.

Pattern Filters and Specific Access Patterns

The messages are scanned to see if they match any existing Pattern Filters and Specific Access Patterns set to **Trust** or **Allow Relaying**.

Trusted and Blocked Senders List

If a sender is on a user’s Trusted Senders List, the message skips all remaining checks. If the sender is on a user’s Blocked Senders List, the message is rejected or discarded.

Content Scanning

Deep scanning is performed on message content and attachments (for example, Microsoft Word or Adobe PDF files) to check for blocked words and phrases.

Document Fingerprinting

Messages are checked by the Document Fingerprinting feature to examine message attachments against an uploaded training set of allowed and forbidden documents.

Content Rules

If enabled, any defined Content Rules are applied to the message.

Encryption

If enabled, outbound messages are encrypted before being delivered.

Anti-Spam Processing

If the message arrives from an untrusted source, it is processed for spam by the Intercept Anti-Spam engine. All Intercept components that are enabled contribute to the final spam score of a message.

Mail Mappings

The message is accepted for processing and these actions occur:

- If the recipient address is not for a domain or sub-domain for which the system is configured to accept mail (either as an inbound mail route or a virtual domain), then the message is rejected.
- If the recipient address is mapped in the Mail Mappings table, then the To: field in the message header is modified as required.

Virtual Mappings

The message is examined for a match in the Virtual Mapping table. If a mapping is found, the envelope-header recipient field is modified as required. LDAP virtual mappings is then processed. Virtual mappings are useful for these situations:

Acting as a wildcard mail mapping. For example, any message for a user at example.com goes to exchange.example.com. You can create exceptions to this rule in the mail mappings for particular users.

ISPs that need to accept mail for several domains and the envelope-header recipient field needs to be rewritten for further delivery.

To deliver to internal servers, define a mail route in **Configuration > Mail > Routing**.

Relocated Users

When mail is sent to an address that is listed in the relocated user table, the message is bounced back with a message informing the sender of the relocated user’s new contact information.

Mail Aliases

When mail needs to be delivered locally, the local delivery agent runs each local recipient name through the aliases database. An alias results in the creation of a new mail message for the named address or addresses. This mail message is then processed again by the system to be mapped and routed. This process also occurs with local user accounts that have a forwarder address configured. Local user accounts are treated like aliases in this case.

Local aliases are typically used to implement distribution lists or to direct mail for standard aliases, for example, mail directed to the postmaster account. LDAP aliases are then processed. LDAP functionality can be used to search for mail aliases on directory services, for example, Active Directory.

Mail Routing

During the mail routing process, there is no modification made to the mail header or the envelope.
A mail route specifies this information:

- The email domains for which the WatchGuard XCS accepts mail (other than itself)
- The hosts to which to deliver the mail

Message Delivery

The message has passed all security and content processing, and is delivered to its destination.

Message Processing Order Summary

This list summarizes the full order in which incoming messages are processed by the WatchGuard XCS:

SMTP Connection Checks

- Reject on Threat Prevention
- Reject on missing addresses
- Reject if number of recipients exceeds maximum
- Reject if message size exceeds maximum
- Reject on unauth SMTP pipelining
- Reject on expired license
- Reject on Specific Access Pattern and Pattern Filter HELO
- Reject on Specific Access Pattern and Pattern Filter Envelope-To
- Reject on Specific Access Pattern and Pattern Filter Envelope-From
- Reject on Specific Access Pattern and Pattern Filter Client IP
- Connection Rules
- Reject on DNS Block List (DNSBL)
- Reject on Reputation Enabled Defense reputation
- Reject on Reputation Enabled Defense infected
- Reject on Reputation Enabled Defense dial-up

At this point, local and trusted networks (this includes Specific Access Pattern Trust), skip any remaining Reject checks.

- Reject on Backscatter Detection
- Reject on unknown sender domain
- Reject on missing reverse DNS
- Reject on missing sender MX
- Reject on non-FQDN sender
- Reject on unknown recipient

Message Checks

- Very Malformed
- Anti-Virus
- Spyware detection
- Pattern Filter Bypass (This action skips remaining checks)
- Attachment Size Limits
- Malformed messages
- Attachment Control (Block)
- Attachment Control (Strip: message continues to be processed for other checks)
- Outbreak Control

- Objectionable Content Filtering
- Pattern Filter (High priority)
- Pattern Filter (Medium priority)
- Trusted Senders List (Skips remaining checks)
- Blocked Senders List
- Pattern Filter (Low priority)
- Content Scanning
- Document Fingerprinting
- Content Rules
- Specific Access Patterns (Trusted bypasses Anti-Spam and allows mail relay)
- Message Encryption (Trusted Only)
- Trusted Network (Skips remaining checks)
- Brightmail (Only if the Brightmail mode is set to "Perform Brightmail Actions".

Intercept Anti-Spam Processing

- SPF (Sender Policy Framework)
- DomainKeys
- DNS Block Lists
- Mail Anomalies
- Spam Words
- Reputation Enabled Defense Reputation
- Reputation Enabled Defense Dial-up
- Token Analysis
- Backscatter Detection
- Brightmail (if configured to integrate with Intercept)
- URL Block Lists

Message Mappings and Routing

- Mail Mappings
- Virtual Mappings
- Relocated Users
- Mail Aliases
- Mail Routing
- Message delivery to its final destination

2 Getting Started

Before You Begin

Before you begin the installation process, make sure you do the tasks described in the subsequent sections.

Verify Basic Components

Make sure that you have:

- A computer with an Ethernet network interface card and a web browser installed
- A WatchGuard XCS device
- Ethernet cables
- Power cables

You can also attach an optional monitor and keyboard (USB or PS/2) to get access to the WatchGuard XCS console.

Hardware Installation

For detailed instructions on how to install the WatchGuard XCS device in an equipment rack, see the *Hardware Guide*.

Physical Location

To safely install your WatchGuard XCS device, we recommend you select a physical location that meets these specifications:

- Install the device in a secure location, for example, in a locked equipment rack or a secure server room.
- Make sure that the network connections are secure, and the network hubs and switches are in the same secure location. Any network patch cables should be of the appropriate length (as short as possible).

- If a monitor and keyboard are attached to the device for console use, make sure that keystroke logging devices cannot be added to the keyboard connection. Connect the monitor and keyboard directly to the device.
- Use the Web UI only in a secure location at a trusted workstation. Do not use the Web UI in any location where the administrative session can be monitored physically or electronically.

Connect the Network Interfaces

Before installation, make sure that you physically connect at least one of the network interfaces to the network.

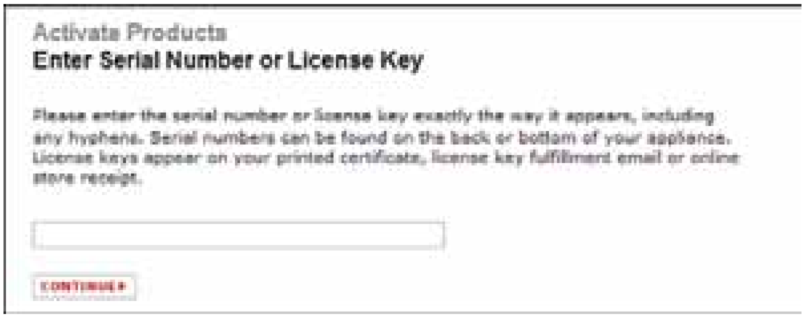
When you install your device, we recommend you use the first onboard Ethernet network interface at the left of the device (NIC 1) to connect to your network. This is the first default interface assigned by the WatchGuard XCS. After you complete the installation, you can configure additional network interfaces.

Get a Feature Key from LiveSecurity

A feature key is a license that enables you to activate your purchased feature set on your WatchGuard XCS. You must register the device serial number on the WatchGuard LiveSecurity web site and retrieve your feature key before adding it to the WatchGuard XCS.To retrieve a feature key from the LiveSecurity web site:

> ***Note*** *Make sure you can access the Internet if the device is installed behind a network firewall, or connects through an external proxy server.*

1. Open a web browser and go to https://www.watchguard.com/activate.
2. If you have not already logged in to LiveSecurity.
   The LiveSecurity Log In page appears.
3. Enter your LiveSecurity user name and password.
   The Activate Products page appears.



Activate Products

Enter Serial Number or License Key

Please enter the serial number or license key exactly the way it appears, including any hyphens. Serial numbers can be found on the back or bottom of your appliance. License keys appear on your printed certificate, license key fulfillment email or online store receipt.

4. Enter the serial number for the product as it appears on your hardware device, including the hyphens.
5. Click **Continue**.
   The Choose Product to Upgrade page appears.
6. In the drop-down list, select the WatchGuard XCS device.
7. Click **Activate**.
   The Retrieve Feature Key page appears.
8. Copy the full feature key to a text file and save it on your computer.
9. Click **Finish**.

Gather Network Addresses

Before you start the installation, make sure you have this information about your network:

Hostname

The hostname assigned to the WatchGuard XCS. For example, if the FQDN (Fully Qualified Domain Name) is hostname.example.com, use `hostname`.

Domain Name

The domain name associated with the assigned hostname. This is the domain to which messages are sent. For example, `example.com`.

Internal IP Address

Select an IP address for the internal network interface. You use this address to connect remotely to the XCS device with a web browser.

External IP Address

Select an IP address for the external network interface (if required). This is the external interface that connects to a public network, such as the Internet.

Subnet Mask

The subnet mask for the IP addresses you selected.

Gateway Address

The default gateway for the XCS device. This is usually your network router.

Mail Domains

The mail domains for which the WatchGuard XCS processes messages.

Optional Network Cards

The IP address, Subnet Mask, and Gateway Address for any additional network cards required by your deployment.

DNS Servers

The addresses of your DNS (Domain Name Service) name servers. We recommend that you include both a primary and a secondary server.

NTP Servers

The addresses of your NTP (Network Time Protocol) servers for time synchronization. We recommend that you include both a primary and a secondary server.

Table 1: Basic Network Settings		Example
Hostname	______________________	hostname
Domain Name	______________________	example.com

Table 1: Basic Network Settings		Example
Internal IP Address	_____._____._____._____	10.0.0.1
Subnet Mask	_____._____._____._____	255.255.255.0
External IP Address	_____._____._____._____	100.100.100.10
Subnet Mask	_____._____._____._____	255.255.0.0
Gateway Address	_____._____._____._____	10.0.0.2
Mail Domains	_____________________ _____________________ _____________________	example.com example1.com
Internal Mail Servers	_____._____._____._____ _____._____._____._____ _____._____._____._____	10.0.2.25 10.0.3.25
Optional Network Cards	_____._____._____._____ _____._____._____._____	10.0.5.10
DNS Servers	_____._____._____._____ _____._____._____._____	10.0.2.53 10.0.3.53

Table 1: Basic Network Settings		Example
NTP Servers	_____._____._____._____ _____._____._____._____	10.0.2.123 10.0.3.123

DNS Configuration for Mail Routing

DNS services are used to route mail messages from the Internet to the WatchGuard XCS. DNS configurations can be complex and are dependant on your specific networking environment.

These instructions represent the minimum changes required to facilitate mail routing.

Add an MX (mail exchanger) record to your DNS configuration to forward incoming messages to the WatchGuard XCS:

```
example.com. IN MX 0 hostname.example.com
```

Add an A record to resolve the domain name to an IP address:

```
hostname.example.com. IN A 10.0.0.1
```

Add a PTR record to allow reverse look-ups to succeed and prevent messages sent from the WatchGuard XCS from being marked as suspected spam:

```
1.0.0.10.in-addr.arpa. IN PTR hostname.example.com
```

Consider keeping an MX record with a higher preference pointed at your current mail server during the integration phase. If the WatchGuard XCS is taken out of service, the messages automatically routes directly to the mail server. This entry should be deleted before you move to a production environment because spammers could find this alternate route and bypass the WatchGuard XCS.

```
example.com. IN MX 10 mailserver.example.com
```

Network Firewall Configuration

To enable the WatchGuard XCS to effectively process messages when it is located behind a network firewall, you must correctly configure the network ports on your network firewall.

This table describes the ports required for each feature. If you do not use a feature in the table, you do not have to open the port for that feature:

Port	Description	From Internet	To Internet	From Internal Network	To Internal Network	Protocol
21	FTP for System Backups				X	TCP
22	SCP (Backup or Offload)				X	TCP
25	SMTP (standard port for sending and receiving of mail)	X	X	X	X	TCP

Port	Description	From Internet	To Internet	From Internal Network	To Internal Network	Protocol
53	DNS and RED Queries		X		X	TCP/UDP
80	Anti-Virus Updates (also requires port 443)		X			TCP
80	URL Categorization Updates		X			TCP
80	Web Mail Access (OWA, iNotes, etc.) See port 443 for Secure WebMail access.	X		X		TCP
110	POP3	X		X		TCP
123	Network Time Protocol (NTP)		X		X	UDP
143	IMAP Proxy	X		X		TCP
161	SNMP			X		UDP
162	SNMP trap				X	UDP
389	LDAP				X	TCP
443	Software Updates		X			TCP
443	Anti-Virus Updates (also requires port 80)		X			TCP
443	Secure Web Mail Access	X		X		TCP
443	Web UI connections	X		X		TCP
443	SecureMail Email Encryption		X			TCP
443	RED Statistics Sharing		X			TCP
443	Brightmail updates		X			TCP
514	Syslog				X	UDP
636	LDAPS				X	TCP
993	Secure IMAP	X		X		TCP
995	Secure POP3	X		X		TCP
1812	RADIUS Server				X	UDP
5500	RSA Secure ID ACE Server				X	UDP
10101	Support Access	X	X			TCP
10106	Centralized Management	X	X	X	X	TCP
10108	Web Reputation		X			UDP

Modify Internal Mail Servers for Outbound Mail

Changes are required to your existing internal mail servers to route outbound mail through the WatchGuard XCS. You must configure your internal mail servers to use the hostname or IP address of the XCS device for SMTP delivery of outbound mail. The procedure depends on the type of internal mail server you use. See the instructions for your specific mail server to route outgoing mail through the WatchGuard XCS.

The instructions below are for a Microsoft® Exchange mail server.

Exchange 2000 and 2003

To add the WatchGuard XCS to the outbound configuration on an Exchange 2000 or Exchange 2003 server:

1. Open Exchange System Manager.
2. Select **Connectors**.
3. Go to the **Internet Mail SMTP Connector**.
4. Select the **Forward all mail through this connector to the following smart hosts:** option.
5. Type the IP address of your WatchGuard XCS system in square brackets.

   For example, `[10.0.1.25]`

   To add multiple systems, separate them with commas.

   For example, `[10.0.1.25],[10.0.2.25]`
6. Click **OK**.

Multiple Exchange Server Configuration

In an environment with multiple Microsoft Exchange servers (not in a clustered configuration), you must configure each system to route outbound mail through the WatchGuard XCS. This can be performed on a per-server basis with the SMTP connector configuration on each server.

To provide a more efficient configuration, add an *SMTP Connector* to the **Exchange Routing Groups** configuration instead of the **Servers** configuration item. The Routing Group configuration applies to all your Exchange servers.

To configure the SMTP Connector in a routing group of Exchange servers:

1. Open the Exchange System Manager.
2. Select **Routing Groups**.
3. Select the **First Routing Group**.
4. Select **Add**.
5. Select **SMTP Connector**.
6. Type a name for the SMTP Connector.

   For example, `XCSConnector`.
7. Select the **Forward all mail through this connector to the following smart hosts:** option.
8. Type the IP address of your WatchGuard XCS system in square brackets.

   For example, `[10.0.1.25]`

   To add multiple systems, separate them with commas.

   For example, `[10.0.1.25],[10.0.2.25]`

9. In the **Local bridgeheads** section, click **Add**.
10. Add each Exchange server that must send mail through the WatchGuard XCS to the list.

    Make sure you add all servers and not just the primary Bridgehead server.
11. Select the **Address Space** configuration tab.
12. Use the default values of **Type: SMTP**, **Address: ***, and **Cost: 1**.
13. Click **OK**.

Exchange 2007 and 2010

To add the WatchGuard XCS to the outbound configuration on an Exchange 2007 or Exchange 2010 server:

1. Open the Exchange Management Console.
2. Expand the **Organization Configuration** option.
3. Select **Hub Transport**.
4. Select the **Send Connectors** tab.
5. Right-click on the existing **Send Connector**.
6. Select **Properties**.
7. Go to the **Network** tab.
8. Select **Route mail through the following smart hosts:**.
9. Click **Add**.
10. Type the IP address of the WatchGuard XCS system to forward outbound mail to, such as:

    `10.0.1.25`

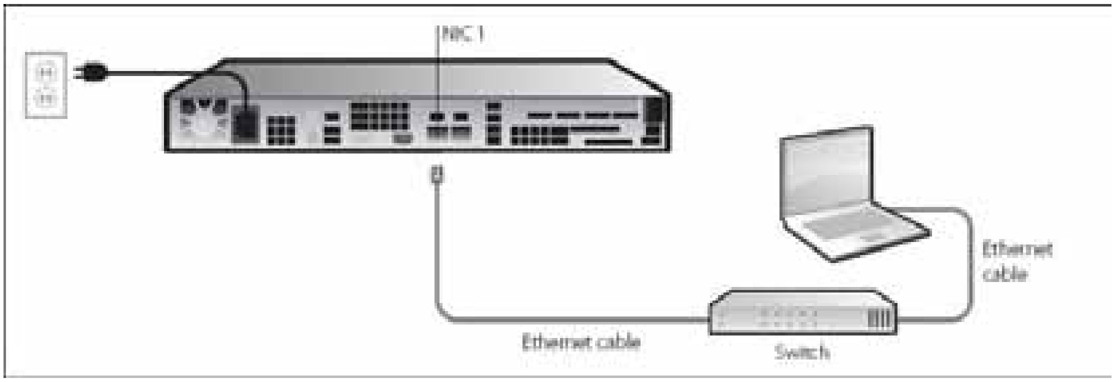
    Repeat this procedure to add the addresses of all of your WatchGuard XCS systems.
11. Click **OK**.

3 Installation

Connect the WatchGuard XCS

To connect the WatchGuard XCS:

1. Unpack the device, cables, and documentation from the shipping carton.
2. Connect the power cable to the system and a power source, preferably a UPS (Uninterruptible Power Supply).
3. Connect the first onboard Ethernet network interface on the left of the device (NIC 1) to the network.
   For the initial installation, you only need to connect the internal network interface to be able to connect to the device with a web browser. You can configure additional network interfaces after the installation.
4. Use one of these methods to get access to the Web UI Installation Wizard:
   - Connect your computer to the same network as the WatchGuard XCS through a network switch.
   - Connect the WatchGuard XCS to the network switch using the first onboard Ethernet connector (NIC 1) at the left side of the back panel.



5. Connect your computer directly to the WatchGuard XCS with a cross-over Ethernet cable connected to the first onboard Ethernet connector (NIC 1) at the left side of the back panel.

Default Network Settings

The default network settings for the WatchGuard XCS are:

- IP address: 10.0.0.1
- Netmask: 255.255.255.0
- Gateway: 10.0.0.2

To connect to the WatchGuard XCS Web UI, we recommend you configure your computer to use the IP address 10.0.0.2.

The WatchGuard XCS supports these web browsers:

- Internet Explorer 7 (Windows XP, Windows 2000, Windows 2003, Windows Vista, Windows 7)
- Internet Explorer 8 (Windows XP, Windows 2000, Windows 2003, Windows Vista, Windows 7)
- Firefox 3 and greater (Windows, Linux, Mac)

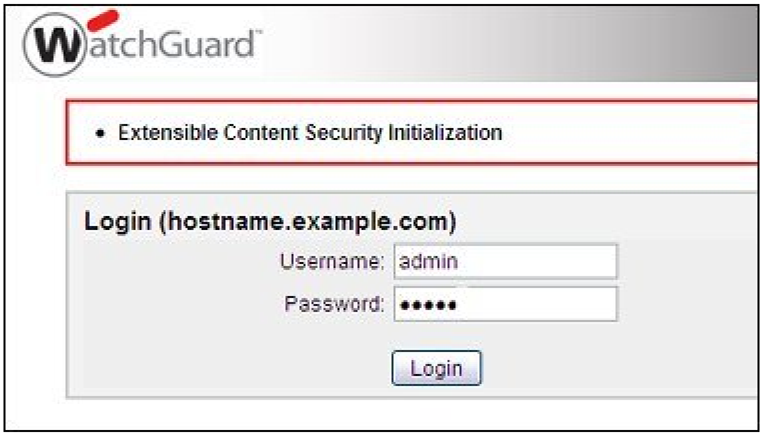
Use a minimum screen resolution of 1024x768.

Start the Installation Wizard

1. Power on your device.

   Wait at least 5 minutes for the system to initialize before you try to connect to the WatchGuard XCS with a web browser. Ping is enabled on the configured network interface. You can ping the default address 10.0.0.1 to check connectivity before you connect with a web browser.

2. Launch a web browser on your computer and type the IP address of the WatchGuard XCS as the URL in the location bar. For example, `https://10.0.0.1`
   The login page appears.



- Extensible Content Security Initialization

Login (hostname.example.com)

Username: admin

Password: •••••

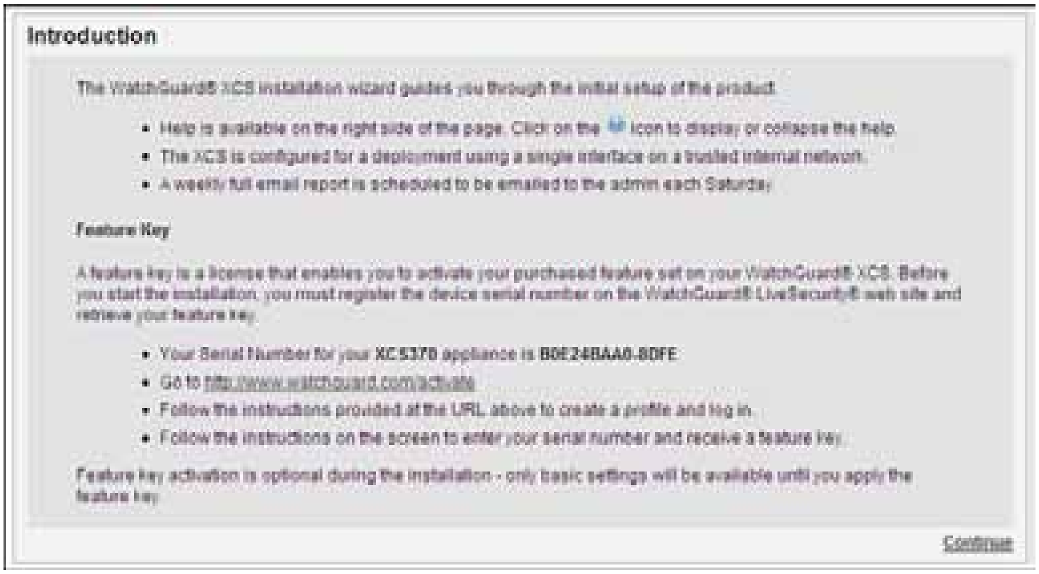
> ***Note*** *A security certificate notification appears in the browser because the system uses a self-signed certificate. It is safe to ignore the warning (Internet Explorer) or to add a certificate exception (Mozilla Firefox).*

3. Type the default **Username** and **Password**.

   When you access the system for the first time after installation, the default settings are **admin** for the username, and **admin** for the password.

4. The Installation Wizard introduction page appears. Click **Continue** to start the installation.

   Make sure you register your device serial number with the WatchGuard® LiveSecurity® web site and receive a feature key before you continue with installation.



Introduction

The WatchGuard® XCS installation wizard guides you through the initial setup of the product.

- Help is available on the right side of the page. Click on the icon to display or collapse the help.
- The XCS is configured for a deployment using a single interface on a trusted internal network.
- A weekly full email report is scheduled to be emailed to the admin each Saturday.

Feature Key

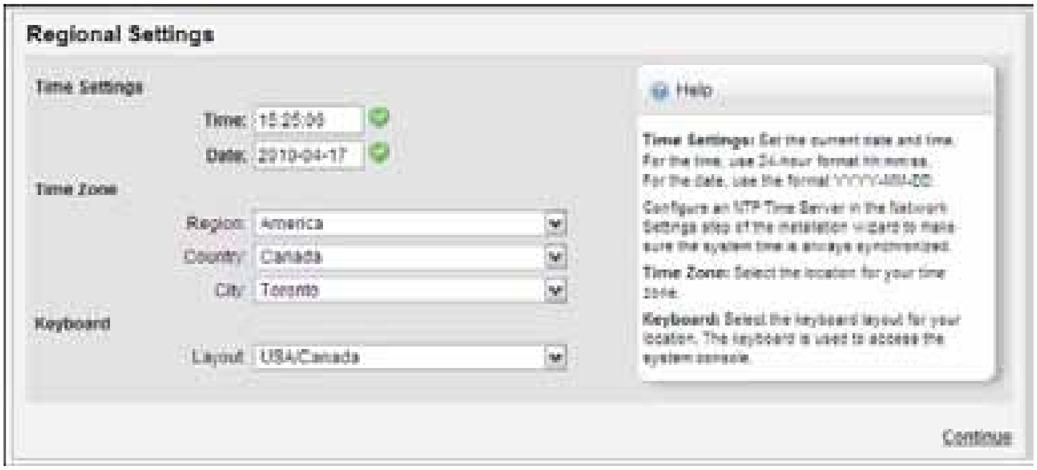
A feature key is a license that enables you to activate your purchased feature set on your WatchGuard® XCS. Before you start the installation, you must register the device serial number on the WatchGuard® LiveSecurity® web site and retrieve your feature key.

- Your Serial Number for your **XCS370** appliance is **B0E24BAA0-8DFE**
- Go to http://www.watchguard.com/activate
- Follow the instructions provided at the URL above to create a profile and log in.
- Follow the instructions on the screen to enter your serial number and receive a feature key.

Feature key activation is optional during the installation - only basic settings will be available until you apply the feature key.

5. In the **Regional Settings** page, configure these options:

   - **Time Settings** – Type the current **Time** and **Date**. For the time, use 24-hour format hh:mm:ss. For the date, use this format: YYYY-MM-DD.
   - **Time Zone** – Select the closest city to your location and time zone.
   - **Keyboard** – Select the keyboard layout for your location. You can attach a keyboard and monitor to the WatchGuard XCS to get access to the console.



Regional Settings

Time Settings

Time: 15:25:36

Date: 2010-04-17

Time Zone

Region: America

Country: Canada

City: Toronto

Keyboard

Layout: USA/Canada

Help

Time Settings: Set the current date and time. For the time, use 24-hour format hh:mm:ss. For the date, use the format YYYY-MM-DD.

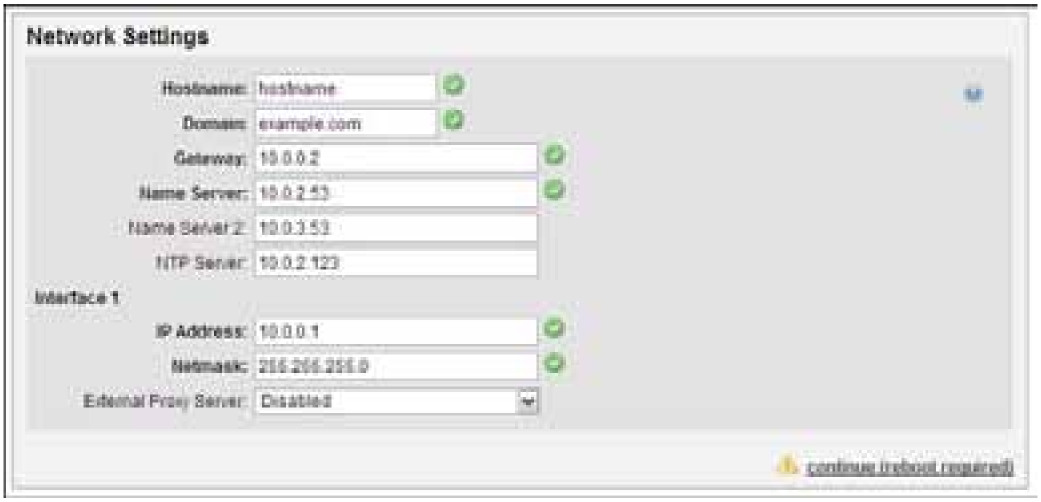
Configure an NTP Time Server in the Network Settings step of the installation wizard to make sure the system time is always synchronized.

Time Zone: Select the location for your time zone.

Keyboard: Select the keyboard layout for your location. The keyboard is used to access the system console.

6. Click **Continue**.
7. On the **Networks Settings** page, configure the first network interface.

   This is the first onboard Ethernet connector (NIC 1) at the left side of the back panel of your device.



Network Settings

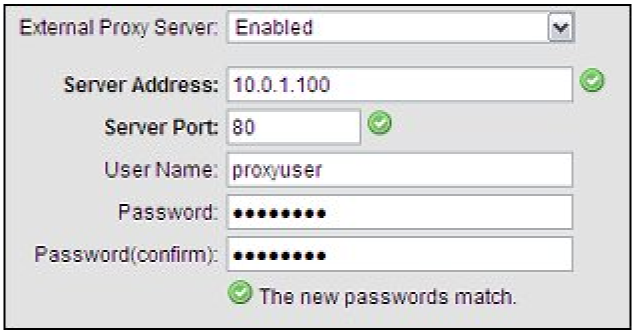
Hostname: hostname ✓
Domain: example.com ✓
Gateway: 10.0.0.2 ✓
Name Server: 10.0.2.53 ✓
Name Server 2: 10.0.3.53
NTP Server: 10.0.2.123

Interface 1

IP Address: 10.0.0.1 ✓
Netmask: 255.255.255.0 ✓
External Proxy Server: Disabled

You can configure these options:

- **Hostname** – Type the hostname for the device.
  For example, if your fully qualified domain name is hostname.example.com, type `hostname`.
- **Domain** – Type your domain.
  For example, type `example.com`.
- **Gateway** – Type the gateway (typically the router) for your network.
  For example, type `10.0.0.2`.
- **Name Server** – Type the IP address of your DNS Name Server.
  For example, type `10.0.2.53`.
- **Name Server 2** – Type the IP address of a secondary DNS name server.
  For example, type `10.0.3.53`.
- **NTP Server** – Type the IP address or hostname of your NTP server.
  For example, type `10.0.2.123`.
- **IP Address** – Type IP address for this interface.
  For example, type `10.0.0.1`.
- **Netmask** – Type the netmask.
  For example, type `255.255.255.0`.
- **External Proxy Server** – If your network uses a proxy server to access the Internet, you must set this option to **Enabled** and enter your external proxy server configuration. The WatchGuard XCS requires access to the Internet through the proxy server to retrieve license information and software updates. If you do not use an external proxy server, keep this option set to **Disabled**.



External Proxy Server: Enabled
Server Address: 10.0.1.100 ✓
Server Port: 80 ✓
User Name: proxyuser
Password: ●●●●●●●●●
Password(confirm): ●●●●●●●●●
✓ The new passwords match.

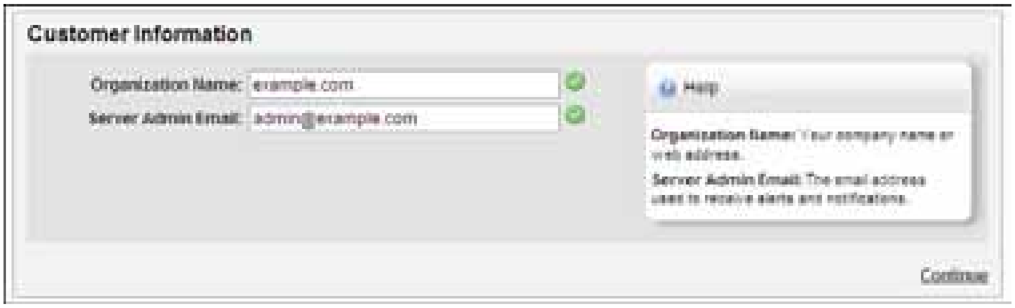
- **Server Address** – Type the IP address of your external proxy server.
- **Server Port** – Type the server port used by the external proxy server. The default is TCP port 80.
- **User Name** – If your proxy server requires authentication, type the user name to log in to the proxy server.
- **Password** – Type and confirm a password.

8. Click **Continue**.

   If you make any network changes, you must restart the device and reconnect to the WatchGuard XCS with the new IP address you assigned to the network interface.

> **Note** *Make sure your computer is configured to get access to the new IP address settings on the WatchGuard XCS.*

9. On the **Customer Information** page, type the **Organization Name** and **Server Admin Email**.
   Device alerts and notifications are sent to the Server Admin Email address.



Customer Information

Organization Name: example.com

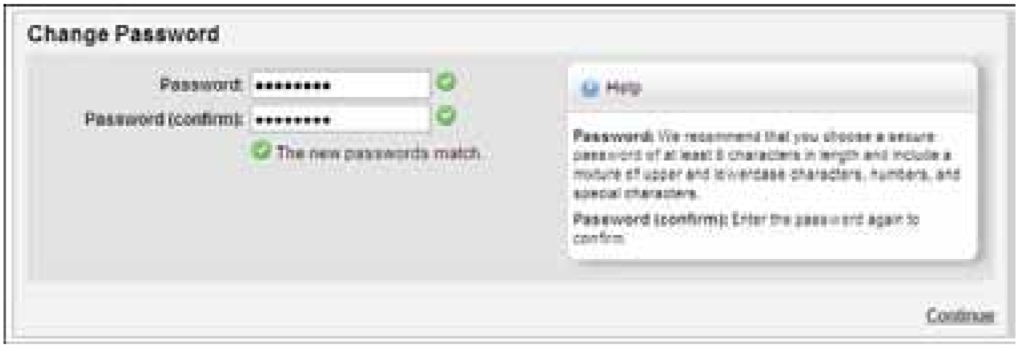
Server Admin Email: admin@example.com

Help

Organization Name: Your company name or web address.

Server Admin Email: The email address used to receive alerts and notifications.

10. Click **Continue**.
11. On the **Change Password** page, type and confirm a new admin password.
    We recommend that you choose a secure password of at least 8 characters in length and include a mixture of upper and lowercase letters, numbers, and special characters.



Change Password

Password: ●●●●●●●●●

Password (confirm): ●●●●●●●●●

The new passwords match.

Help

Password: We recommend that you choose a secure password of at least 8 characters in length and include a mixture of upper and lowercase characters, numbers, and special characters.

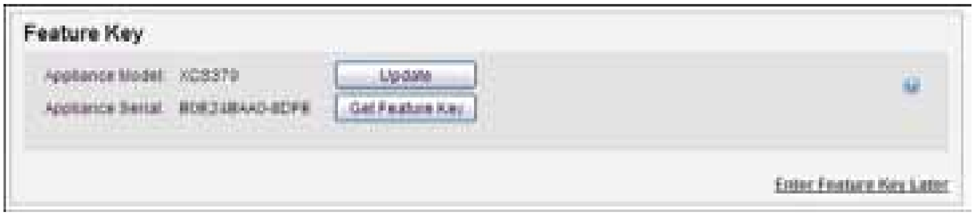
Password (confirm): Enter the password again to confirm.

12. Click **Continue**.
13. On the **Feature Key** page, select one of these options to add your feature key:

- Click **Update** to manually add a feature key. Paste your feature key into the text box and click **Apply**.
- Click **Get Feature Key** to automatically download and apply your feature key from the WatchGuard LiveSecurity service. This option requires an Internet connection and an existing LiveSecurity account. Make sure you can get access to the Internet if the device is installed behind a network firewall, or connects through an external proxy server.

- Click **Enter Feature Key Later** to manually add the feature key after installation. To enter the feature key manually, from the Web UI, select **Administration > System > Feature Key**.

> ***Note*** *If you do not enter a valid feature key in this step, the Mail Configuration and Start Processing steps of the wizard are not displayed.*



Feature Key

Appliance Model: XCS370

Appliance Serial: B0E248AA0-8DF8

If you see errors when you add your feature key, try this:

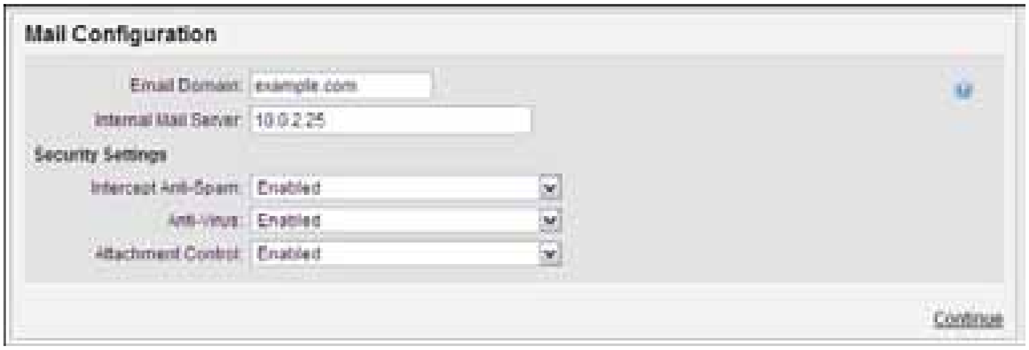
For Automatic Update:

- Make sure you have a valid LiveSecurity account and that you have registered your device serial number.
- You must have an Internet connection to retrieve your feature key.
- Make sure communications are not blocked by a network firewall.

For Manual Update:

- Make sure you cut and paste the entire feature key text.
- The first line must be “Serial Number: B0Exxxxxxxxxx”.
- The last line is a long line that starts with “Signature: “.

17. On the **Mail Configuration** page, type your mail domain and server details, and select the initial status of the WatchGuard XCS security scanning features.



Mail Configuration

Email Domain: example.com

Internal Mail Server: 10.0.2.25

Security Settings

Intercept Anti-Spam: Enabled

Anti-Virus: Enabled

Attachment Control: Enabled

- In the **Email Domain** text box, type the domain for which the WatchGuard XCS processes messages. For example, `example.com`.
- In the **Internal Mail Server** text box, type the IP address of the internal mail server that receives and sends mail through the WatchGuard XCS.

The WatchGuard XCS automatically configures a mail route for the domain and internal mail server you enter on this page. To configure additional domains for mail routing after the installation is complete, from the Web UI, select **Configuration > Mail > Routing**.

The WatchGuard XCS also automatically configures a Specific Access Pattern to trust your internal mail server address to allow the mail server to relay mail outbound through the WatchGuard XCS. Mail that originates from the internal mail server is also trusted for Anti-Spam processing. To configure Specific Access Patterns after the installation is complete, from the Web UI, select **Configuration > Mail > Access**.

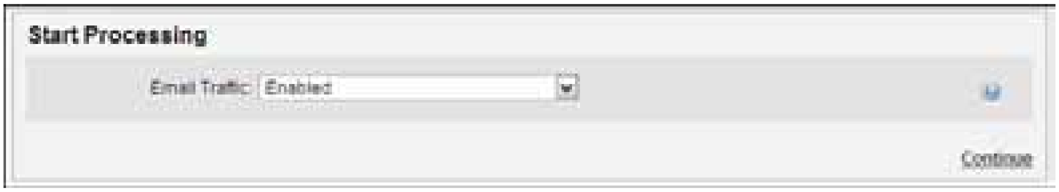
20. In the **Security Settings** section of the **Mail Configuration** page, you can enable or disable **Intercept Anti-Spam**, **Anti-Virus**, and the **Attachment Control** features.

    If you enable these features in the Installation Wizard, mail scanning is active when the installation is complete and mail processing is started.

    When you enable Intercept Anti-Spam, these default *Intercept Settings* take effect.

21. Click **Continue**.
22. From the **Email Traffic** drop-down list, select **Enabled** to start email traffic processing after the installation is complete.

    If you select **Disabled**, you can start mail processing manually from **Activity > Status > Utilities** after the installation is complete.

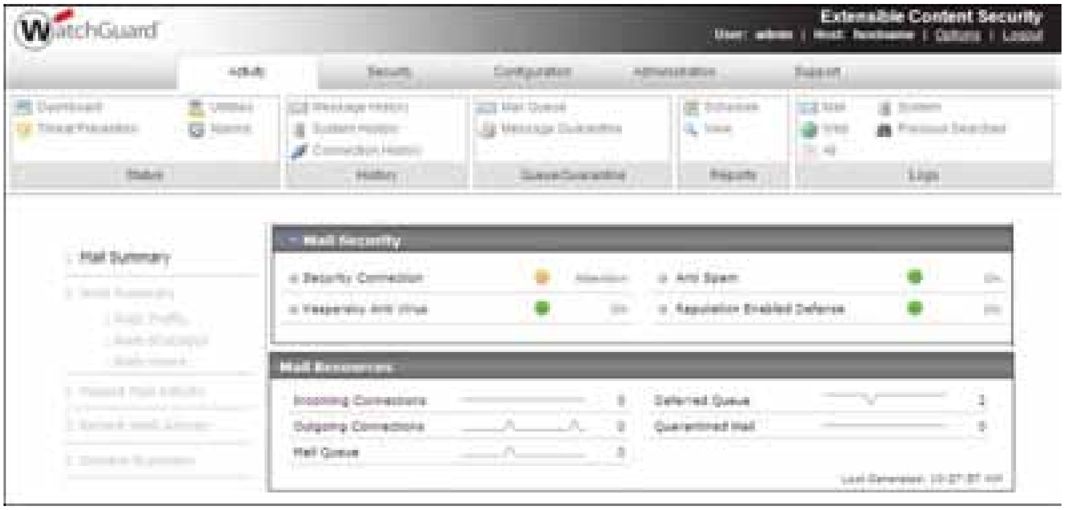


Start Processing

Email Traffic: Enabled

23. Click **Continue**.
24. Click **Done** to complete the installation.
    This process can take up to a minute to complete.

    The main Dashboard appears.



4 Post-Installation Tasks

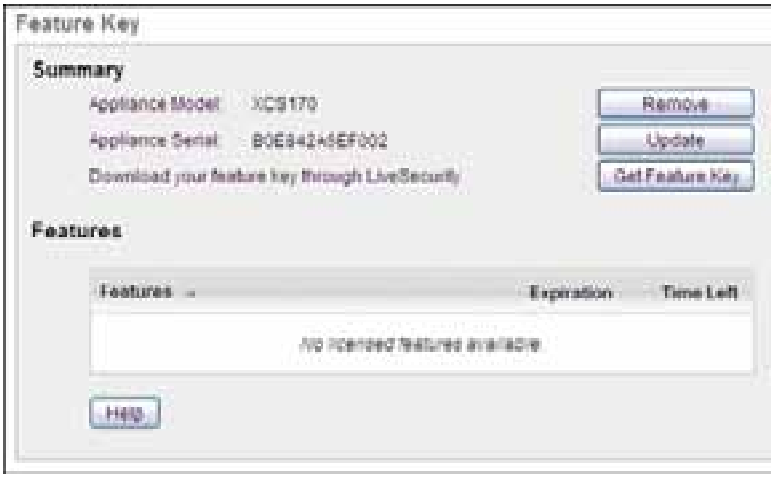
Add a Feature Key

A feature key is a license that enables you to activate your purchased feature set on your WatchGuard XCS. You must register the device serial number on the WatchGuard LiveSecurity web site and retrieve your feature key before adding it to the WatchGuard XCS.

> ***Note*** *Make sure you can access the Internet if the device is installed behind a network firewall, or connects through an external proxy server.*

To install a new feature key:

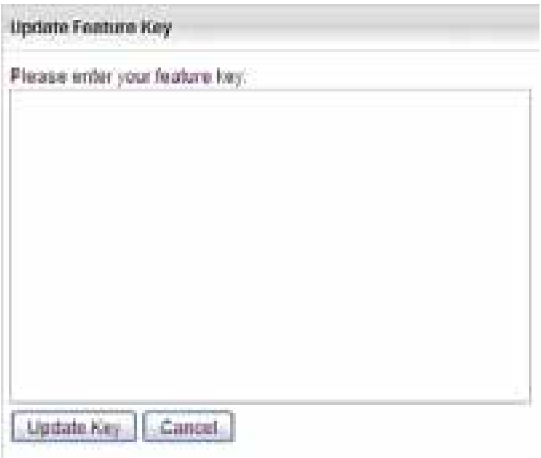
1. Select **Administration > System > Feature Key**.
   The Feature Key page appears.



Appliance Model XCS170
Appliance Serial B0E842A5EF002
Download your feature key through LiveSecurity

No licensed features available

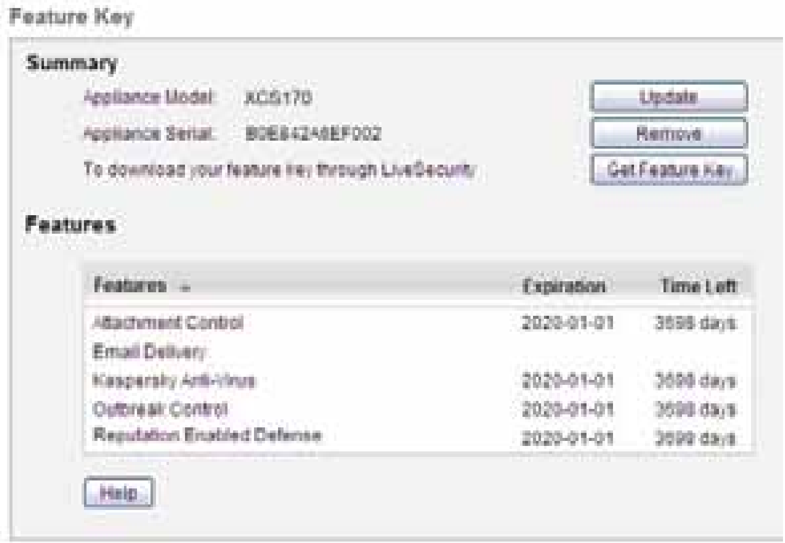
2. Click **Update**.
   The Update Feature Key page appears.



Update Feature Key

Please enter your feature key:

3. Copy the text of the feature key file and paste it in the text box.
4. Click **Update Key**.
   The Feature Key page appears with the new feature key information.



Feature Key

Summary

Appliance Model: XCS170

Appliance Serial: B0E8424AEF002

To download your feature key through LiveSecurity

Features

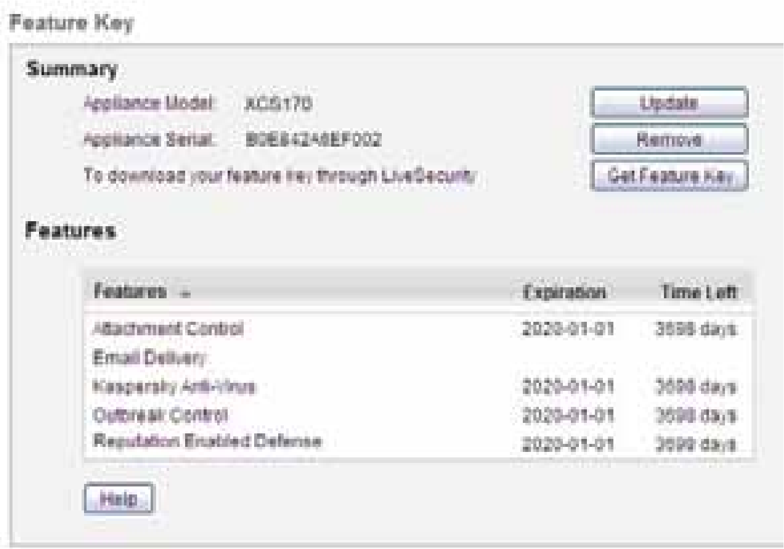
Features	Expiration	Time Left
Attachment Control	2020-01-01	3598 days
Email Delivery		
Kaspersky Anti-Virus	2020-01-01	3598 days
Outbreak Control	2020-01-01	3598 days
Reputation Enabled Defense	2020-01-01	3599 days

Update a Feature Key

If you already have a LiveSecurity login and your WatchGuard device serial number is registered, you can update your feature key automatically from the LiveSecurity site.

To update a feature key:

1. Select **Administration > System > Feature Key**.
   The Feature Key page appears.



Feature Key

Summary

Appliance Model: XCS170

Appliance Serial: B0E842A6EF002

To download your feature key through LiveSecurity

Features

Features	Expiration	Time Left
Attachment Control	2020-01-01	3598 days
Email Delivery		
Kaspersky Anti-Virus	2020-01-01	3599 days
Outbreak Control	2020-01-01	3599 days
Reputation Enabled Defense	2020-01-01	3599 days

2. Click **Get Feature Key**.
   Your feature key is downloaded from the LiveSecurity site and automatically updated on your device.

Troubleshoot Feature Key Updates

If you encounter errors when you add your feature key:

For Manual Update:

- Make sure that you cut and paste the entire feature key text.
- The first line of the feature key must be “Serial Number: B0Exxxxxxxxxx”.
- The last line of the feature key is a long line of characters starting with “Signature: “.

For Automatic Update:

- Make sure you have a valid LiveSecurity account and you have registered your device serial number.
- You must have an Internet connection to retrieve your feature key.
- Make sure communications are not blocked by a network firewall.

Remove a Feature Key

You may need to remove a feature key after an XCS device evaluation or to troubleshoot license issues.

> ***Note*** *If you remove a feature key, you disable all security features and the system stops processing messages.*

To remove an existing feature key:

1. Select **Administration > System > Feature Key**.
   The Feature Key page appears.
2. Click **Remove**.
   A confirmation dialog box appears.
3. Click **OK** to confirm.

Feature Key Expiration

The WatchGuard XCS sends notifications to the administrator at 90, 60, 30, 7, 2, and 1 days before a feature key expires. To make sure your XCS operates with full functionality, update your feature key before the expiration date.

When a feature key expires on the WatchGuard XCS, the device continues to process and deliver mail, but expired features do not scan or perform actions on messages. Also, you will not receive software and Anti-Spam updates from Security Connection.

For example, if the Anti-Virus scanning feature key expires, the WatchGuard XCS continues to process mail, but the messages are not scanned for viruses.

These features do not have associated expiration periods because they are required for normal system operations and management:

- Email
- Clustering
- Queue Replication
- Centralized Management

Security Connection

Security Connection is a service that polls WatchGuard's support servers for new updates, security alerts, and Anti-Spam database updates. The WatchGuard XCS sends a notification to the administrator when new information and updates are available.

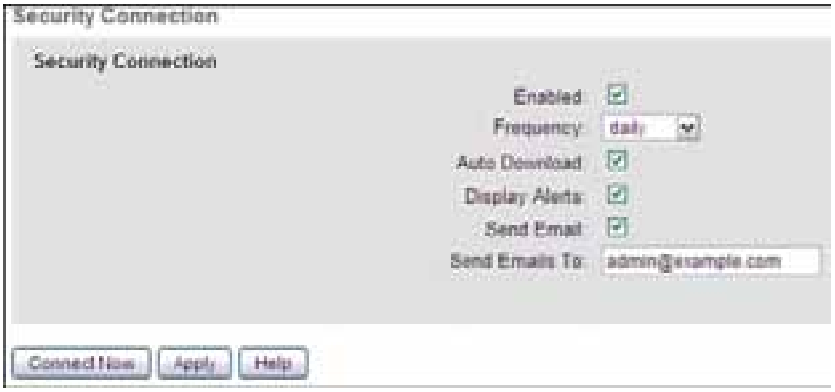
The Security Connection service is enabled by default after you install the WatchGuard XCS to make sure you automatically receive notifications for the latest software updates. After the initial installation, Security Connection immediately checks for new available updates. The Security Connection downloads any available updates for your system, but does not automatically install them.

To install software updates, from the Web UI, select **Administration > Software Updates > Updates**. See *Software Updates* for more detailed information on Software Updates.

> ***Note*** *For security purposes, all Security Connection files are encrypted and contain an MD5-based digital signature that is verified after the file is decrypted.*

To configure Security Connection:

1. Select **Administration > Software Updates > Security Connection**.


Security Connection

Security Connection

Enabled ☑

Frequency daily

Auto Download ☑

Display Alerts ☑

Send Email ☑

Send Emails To admin@example.com

2. Select the **Enabled** check box.
3. From the **Frequency** drop-down list, select how often to run the Security Connection service: **daily**, **weekly**, or **monthly**.
4. To enable software updates to be downloaded automatically, select the **Auto Download** check box.
   Updates are automatically downloaded, but not automatically installed. You must use Software Updates to manually install the updates.
5. To enable Security Connection alert messages to appear on the system console, select the **Display Alerts** check box.
6. To send an email to the address specified in the **Send Emails To** text box, select the **Send Email** check box.
7. In the **Send Emails To** text box, type the email address to receive notifications.
8. Click **Apply**.
9. Click **Connect Now** to run Security Connection and check for new software updates.

Software Updates

To make sure your device software is up to date with the latest patches and upgrades, you must install any updates released for your version of software.

After the installation of the WatchGuard XCS, Security Connection immediately checks for new software and automatically downloads any available updates. The Security Connection does not automatically install these updates. You must manually install them on the **Software Updates** page.

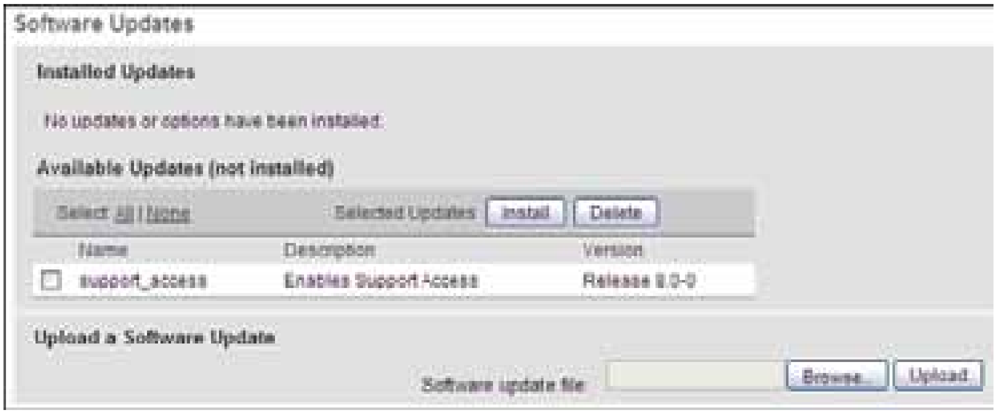
Updates appear in two sections: *Available Updates* (on the device, but not yet installed) and *Installed Updates* (installed and active). You can install an available update, or delete an installed update. Software updates downloaded from Security Connection appear in the *Available Updates* section.

> ***Note*** *We recommend that you back up the current system before you perform a software update. See Backup and Restore for detailed information on the backup and restore procedure.*

Install a Software Update

To install software updates:

1. Select **Administration > Software Updates > Updates**.
   The Software Updates page appears.



Software Updates

Installed Updates

No updates or options have been installed.

Available Updates (not installed)

	Name	Description	Version
□	support_access	Enables Support Access	Release 8.0-0

Upload a Software Update

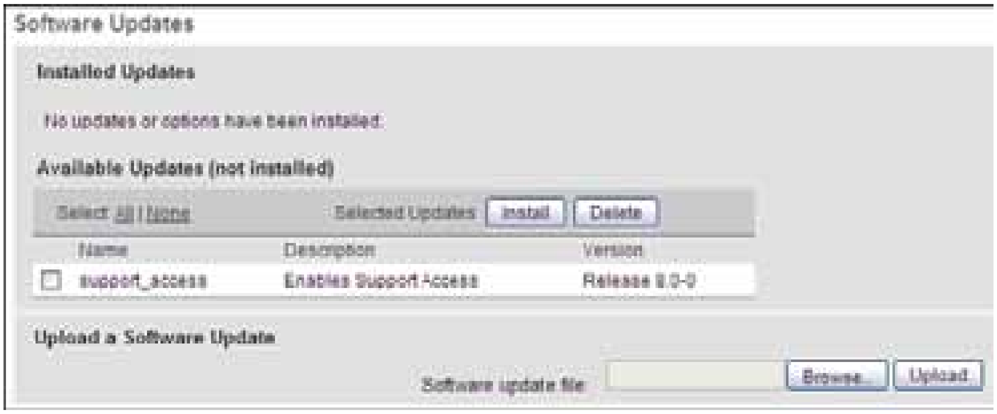
Software update file

2. If you manually downloaded your software update:
   - Click **Browse** and select the software update.
   - Click **Upload**.
     The software update appears in the Available Updates section.
3. In the **Available Updates** section, select the software update.
4. Click **Install**.
   After you install updates, you must restart the device.

Delete a Software Update

To delete software updates:

1. Select **Administration > Software Updates > Updates**.
   The Software Updates page appears.



Software Updates

Installed Updates

No updates or options have been installed.

Available Updates (not installed)

	Name	Description	Version
□	support_access	Enables Support Access	Release 8.0-0

Upload a Software Update

Software update file

2. In the **Installed Updates** section, select the software update to delete.
3. Click **Delete**.
   After you delete the update, you must restart the device.

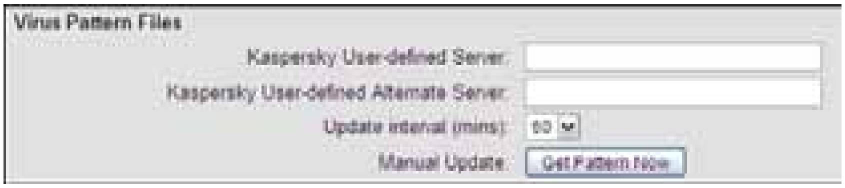
Update Anti-Virus Pattern Files

If licensed, the Anti-Virus service is automatically enabled and started. After the initial installation of the WatchGuard XCS, it may take up to the default of one hour to update your Anti-Virus pattern files to the most recent version. We recommend you update your pattern files immediately after installation.

> ***Note*** *If you access the Internet through a proxy server, you must enter its hostname and port number in the external proxy configuration in* ***Configuration > Network > External Proxy Server*** *for pattern file updates to succeed.*

To update your pattern files:

1. Select **Security > Anti-Virus > Anti-Virus**.



Virus Pattern Files

Kaspersky User-defined Server:

Kaspersky User-defined Alternate Server:

Update interval (mins): 60

Manual Update: Get Pattern Now

2. Go to the **Virus Pattern Files** section.
3. Click **Get Pattern Now**.

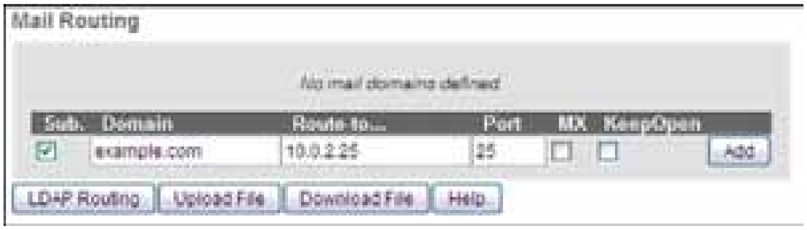
Mail Routing

If you configured a primary email domain and an internal mail server during the initial installation of the WatchGuard XCS, a mail route is automatically set up for that mail server.

Use the *Mail Routing* page to configure additional domains to accept mail for and identify the destination mail servers to route the messages to.

To add and configure mail routes:

1. Select **Configuration > Mail > Routing**.



Mail Routing

No mail domains defined

Sub.	Domain	Route to...	Port	MX	KeepOpen	
☑	example.com	10.0.2.25	25	□	□	Add

2. To accept and relay mail for subdomains of the specified domain, select the **Sub** option.
3. In the **Domain** text box, type the domain for which mail is accepted.

   For example, `example.com`.
4. In the **Route-to** text box, type the IP address for the mail server to which mail is delivered.

   For example, `10.0.2.25`.
5. In the **Port** text box, type the port on which to deliver mail to this server.
   The default is SMTP port 25.

6. If you need to look up the mail routes in DNS before delivery, select the **MX** option.

   If this option is disabled, MX records are ignored. You do not need to select this item unless you are using multiple mail server DNS entries for load balancing and failover purposes. By checking the MX record, DNS sends the request to the next mail server in the list.

7. Select the **KeepOpen** option to make sure that each mail message to the domain is not removed from the active queue until the WatchGuard XCS attempts delivery, even if the preceding mail failed or was deferred.
   This setting makes sure that local mail servers receive high priority.

   > ***Note*** *The KeepOpen option should only be used for domains that are usually very reliable. If the domain is unavailable, it can cause system performance problems because of excessive error conditions and deferred mail.*

8. Click **Add**.
9. Repeat the procedure for any additional domains and mail servers.

Upload Mail Routes

You can upload a list of mail routes in a text file. The file must contain comma or tab separated entries with one entry per line.

Use this format:

```
[domain],[route],[port],[ignore_mx],[subdomains_too],[keepopen]
```

For example:

```
example.com,10.0.2.25,25,on,off,off
```

You must use a text editor to create the file domains.csv.

To update a mail route file:

- To download the mail route list from the WatchGuard XCS, click **Download File**.
- Open the file and update the mail route list.
- Click **Upload File** and upload the edited file to the WatchGuard XCS.

Subdomain Routing with MX Lookup

The WatchGuard XCS can route and deliver messages to subdomains based upon an MX record lookup using the domain portion of the RCPT TO: field of a message.

In the Mail Routing configuration, you can specify “any” or “ANY” in the **Route-to** field. The WatchGuard XCS performs an MX lookup on the specified subdomain, and then the message is delivered based on a DNS A record lookup for the destination host.

When you define the **Route-to** field as “any” or “ANY”, these default values are used, and changing them in the user interface has no effect.

- The default **Port** is 25
- The **MX** option is enabled
- The **KeepOpen** option is disabled

Subdomain Routing and DNS Caching

If DNS caching is enabled, a cached DNS entry can cause a message to be delivered to an incorrect host if the DNS entry is modified. We recommend that you disable the **Enable DNS Cache** option (from **Configuration > Network > Interfaces**) if you use DNS MX lookups for subdomain routing. This can cause a slight decrease in performance of DNS lookups, but makes sure the correct route is used if you change a DNS record.

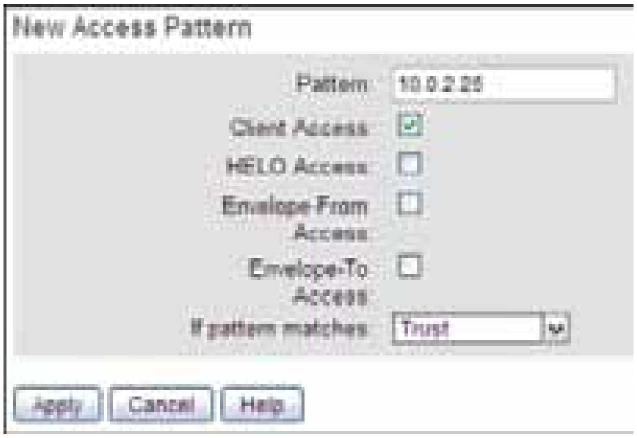
LDAP Routing

Click the **LDAP Routing** button to define mail routes using an LDAP directory server. This is the preferred mail routing method for organizations with a large amount of domains. See *LDAP Routing* for more detailed information on using LDAP for mail routing.

Trust Internal Mail Servers

To allow internal mail systems to relay mail outbound through this WatchGuard XCS, a *Specific Access Pattern* must be set up for the system. A Specific Access Pattern makes sure that your mail servers and their messaging traffic is trusted and not processed for spam.

1. Select **Configuration > Mail > Access**.
2. Click the **Add Pattern** button.



New Access Pattern

Pattern: 10.0.2.25
Client Access ☑
HELO Access □
Envelope-From Access □
Envelope-To Access □
If pattern matches: Trust

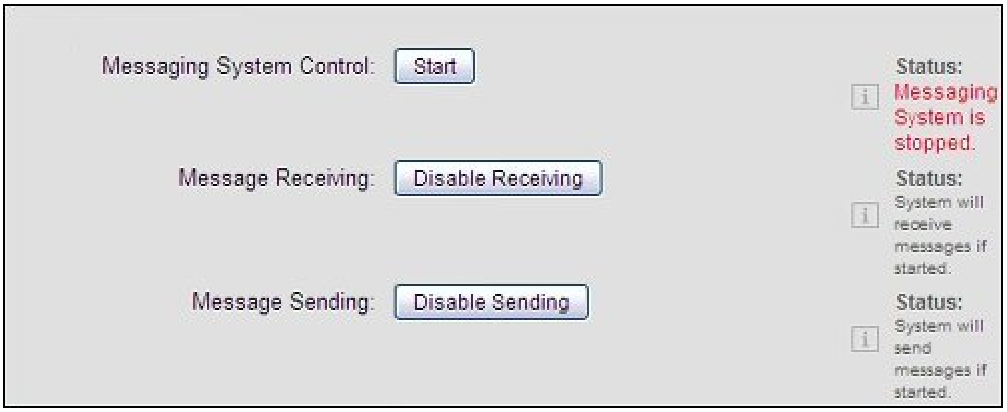
3. In the **Pattern** text box, type the IP address of the client.
4. Select the **Client Access** check box.
5. From the **If pattern matches** drop-down list, select **Trust**.
6. Click **Apply**.

Start Messaging Services

When you have configured the WatchGuard XCS with your required networking information and mail routes, you can start the messaging system and start to process messages.

To start the messaging system:

1. Select **Activity > Status > Utilities**.



Messaging System Control: Start — Status: Messaging System is stopped.

Message Receiving: Disable Receiving — Status: System will receive messages if started.

Message Sending: Disable Sending — Status: System will send messages if started.

2. In the **Messaging System Control** section, click **Start**.
   The status message changes from "Messaging System is stopped" to "Messaging System is running".

5 Administration

Connect to the WatchGuard XCS

You can use these web browsers to connect to the Web UI:

- Internet Explorer 7 (Windows XP, Windows 2000, Windows 2003, Windows Vista, Windows 7)
- Internet Explorer 8 (Windows XP, Windows 2000, Windows 2003, Windows Vista, Windows 7)
- Firefox 3 and greater (Windows, Linux, Mac)

Make sure your screen resolution is set to a minimum of 1024x768.

To administer the WatchGuard XCS with the Web UI:

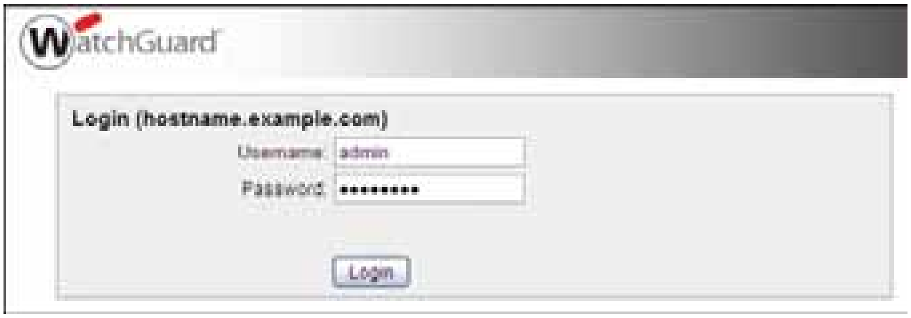
1. Open a web browser and go to the IP address of the WatchGuard XCS.
   For example, `https://10.0.0.1`
   The login page appears.

   > ***Note*** *A security certificate notification appears in the browser because the system uses a self-signed certificate. You can safely ignore the warning (Internet Explorer) or add a certificate exception (Mozilla Firefox).*

2. Type the default **Username** and **Password**.

   When you connect to the device for the first time after installation, the default settings are:

   - Username — **admin**
   - Password — **admin**

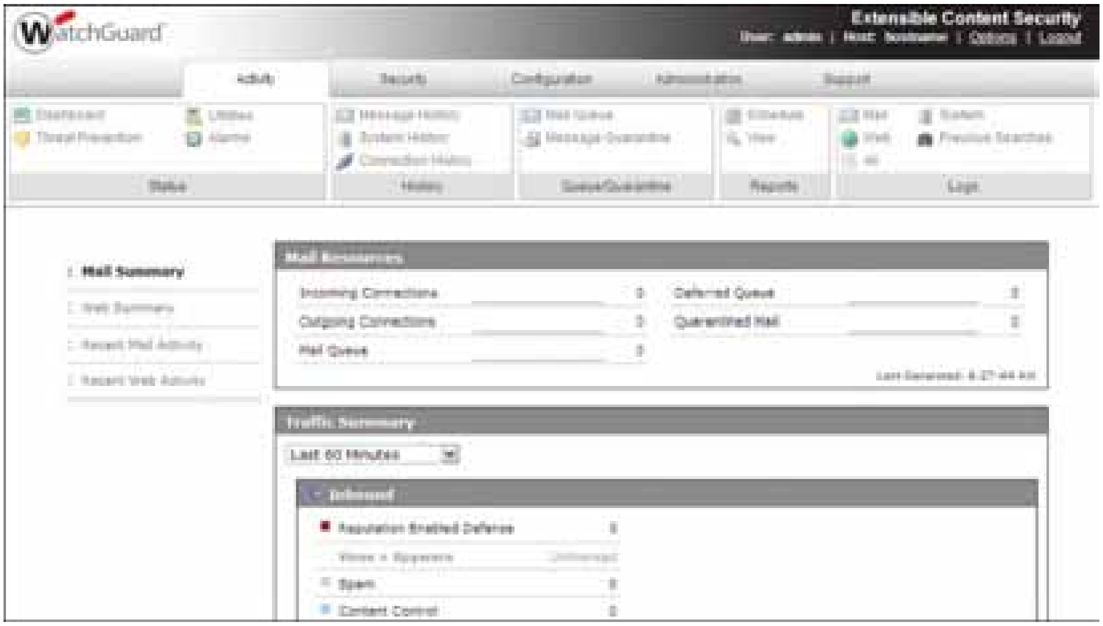


Login (hostname.example.com)

Username: admin

Password: •••••••••

When you log in, the main Dashboard page appears.



Mail Resources

Incoming Connections	0	Deferred Queue	0
Outgoing Connections	0	Quarantined Mail	0
Mail Queue	0		

Last Generated: 8:27:44 AM

Traffic Summary

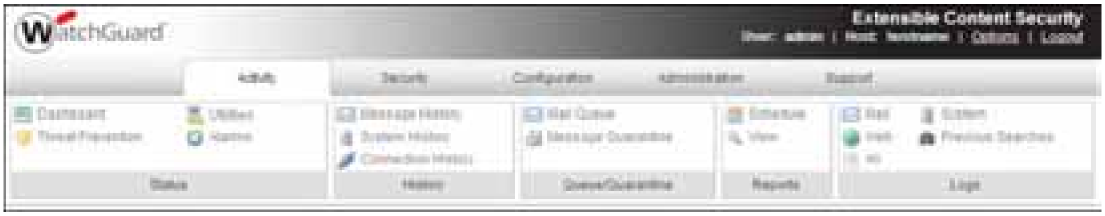
Last 60 Minutes

Inbound

Reputation Enabled Defense	0
Virus + Spyware	Unlicensed
Spam	0
Content Control	0

Navigate the Main Menu

The main menu has these main categories:



> ***Note*** *Depending on your device model and feature package, not all menu configuration items are displayed.*

Activity

The **Activity** menu provides a variety of information on system status and activity. This includes the Dashboard, message history, mail queue and quarantine management, and reports and logs. This menu includes these features:

Status

- Dashboard
- Alarms
- Cluster Alarms (if in a Cluster)
- Cluster Activity (if in a Cluster)
- CM Activity (on a CM Manager only)
- Threat Prevention
- Utilities

History

- Message History
- System History
- Connection History

Queue/Quarantine

- Mail Queue
- Message Quarantine

Reports

- Schedule
- View
- Centralized Management (on a CM Manager only)

Logs

- Mail
- Web
- System
- Previous Searches
- All

Security

Use the **Security** menu to configure the system’s powerful security and content control features.

This menu includes these features:

Anti-Spam

Use the Anti-Spam menu to configure the components of the Intercept Anti-Spam features.

- Anti-Spam
- Intercept Settings
- Connection Control

- Threat Prevention
- Reputation Enabled Defense
- Brightmail (if licensed)

Anti-Virus

The Anti-Virus menu includes message security scanning features, for example, Anti-Virus, Spyware, Outbreak Control, and Malformed Mail scanning:

- Anti-Virus
- Spyware
- Outbreak Control
- Malformed Mail

Encryption

Use the Encryption menu to configure message and delivery encryption features.

- SecureMail
- PostX
- External
- TLS

Content Control

Use the Content Control menu to configure the system’s powerful content control features. This includes Attachment Control, Content Scanning, and other content filters.

- Attachment Control
- Content Scanning
- Objectionable Content
- Document Fingerprinting
- Content Rules
- Pattern Filters
- Dictionaries & Lists
- Custom Actions

Policies

Use the Policies menu to configure system policies for access control and compliance.

- Policies
- User Policy
- Group Policy
- Domain Policy
- IP Policy
- Default Time Policy
- Diagnostics

Configuration

Use the **Configuration** menu to configure device network and mail settings.

This menu includes these items:

Network

Use the Network menu to configure options related to the device's networking features.

- Interfaces
- Virtual Interfaces
- Performance
- Static Routes
- Web Server
- External Proxy Server
- SNMP

LDAP

Use the LDAP menu to configure your Directory Services features that rely on LDAP.

- Directory Servers
- Directory Users
- Web Users
- Aliases
- Mappings
- Recipients
- Relay
- Routing

Mail

Use the Mail menu to configure features related to mail processing and delivery.

- Access
- Delivery
- Routing
- Aliases
- Mapping
- Virtual Mapping
- Archiving
- Domain Keys
- POP3 and IMAP

WebMail

Use the WebMail menu to configure the Secure WebMail and its related features that use the WebMail client.

- WebMail
- Trusted/Block Senders
- User Spam Quarantine

Web

Use the Web menu to configure features specific to the Web Proxy.

- HTTP/S Proxy
- Traffic Accelerator
- Reputation Enabled Defense

- User Reporting
- URL Categorization
- Proxy Auto Configuration
- URL Block Lists

Miscellaneous

Use the Miscellaneous menu to configure the general settings of several features.

- Logs
- Reports
- Customization
- Alarms
- Feature Display

Administration

Use the **Administration** menu to manage the device. This includes user account administration, backup and restore, software updates, and feature key management.

This menu includes these features:

Accounts

Use the User Accounts menu to configure local user accounts and authentication.

- Administrator
- Local Accounts (or Tiered Admin if in a cluster)
- Mirror Accounts
- Delegated Domains
- Relocated Users
- Vacations
- Remote Authentication
- SecurID

Backup/Restore

Use the Backup/Restore menu to backup and restore the device configuration and data.

- Backup & Restore
- Daily Backup

Software Updates

Use the Software Updates menu to manage device software updates and the Security Connection.

- Updates
- Security Connection

Multi-System Management

Use the Multi-System Management menu to configure multi-system features, for example, Centralized Management and mail queue replication.

- Centralized Management
- Configuration Set (if on a CM Manager)

- Entities (if on a CM Manager)
- Entity Status (if on a CM Entity)
- Queue Replication

System

Use the System menu to configure system administrative settings, for example, feature keys and certificates.

- Feature Key
- SSL Certificates
- Regional Settings
- Reboot & Shutdown

Support

Use the **Support** menu to obtain additional support for the product.

This menu includes these features:

- Technical Support
- Problem Reporting
- Reputation Enabled Defense
- Online Access (main Web site)
- Online Manual
- Microsoft Outlook Add-ins

WatchGuard XCS Console

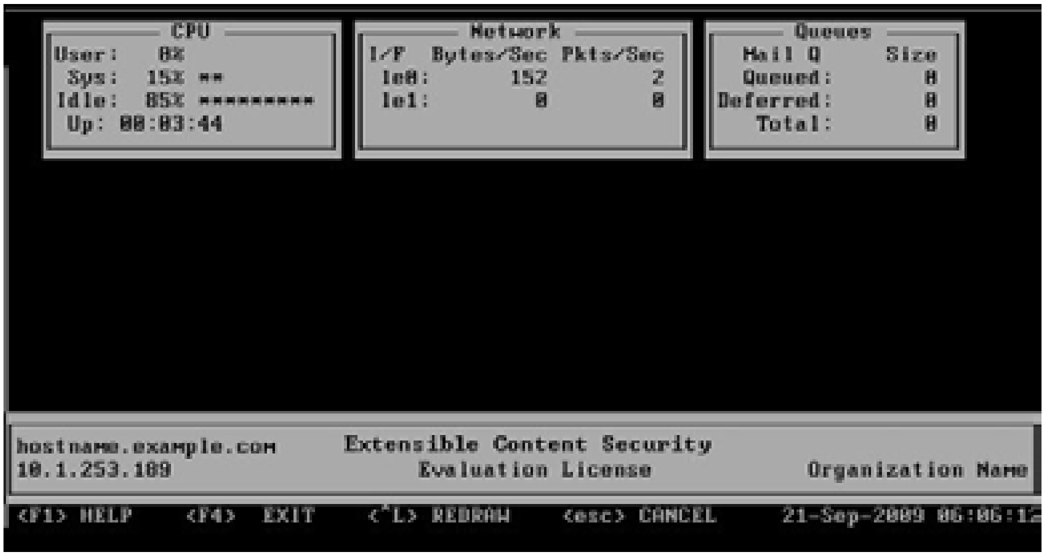
The WatchGuard XCS console supports a limited subset of administrative tasks and should only be used for troubleshooting or for a custom installation. We recommend you perform all routine administration through the Web UI.

When you access the console for the first time after installation, the default login credentials are **admin** for the UserID, and **admin** for the Password. The password can be changed from the Web UI administration interface.

Console Activity Page

The console activity page provides you with basic activity and statistics information for this device.

Press any key to log in to the console with your admin login credentials.



```
            CPU                      Network                    Queues
User:    0%              I/F  Bytes/Sec Pkts/Sec        Mail Q      Size
 Sys:   15% **            le0:       152        2      Queued:         0
Idle:   85% **********    le1:         0        0    Deferred:         0
 Up: 00:03:44                                            Total:         0

hostname.example.com      Extensible Content Security
10.1.253.189                    Evaluation License              Organization Name
<F1> HELP    <F4>   EXIT    <^L> REDRAW    <esc> CANCEL     21-Sep-2009 06:06:12
```

Admin Menu

The **Admin** menu contains these options:

- **Exit** – Exits the console.
- **Hardware Information** – Displays the processor type, available memory, and network interface information.
- **Configure Interfaces** – Allows you to modify the host and domain name, IP address, Gateway, DNS and NTP servers for all network interfaces.
- **Security Connection** – Enables automatic software updates.
- **Shutdown** – Shuts down the device.
- **Reboot** – Shuts down and restarts the device.

Diagnostics Menu

The **Diagnostics** menu contains these options:

- **Activity Display** – Displays CPU usage, network traffic and mail message activity.
- **Ping** – Allows you to test network connectivity to other systems with the ping utility.
- **Traceroute** – Displays the routing steps between the device and a destination host.
- **Reset Network Interface** – Resets network interfaces. This function is useful to correct connection issues.
- **Display Disk Usage** – Displays the amount of used and available disk space.
- **Display System Processes** – Displays information about processes running on the system.

Repair Menu

The **Repair** menu contains these options:

- **Reset SSL Certificates** – Sets certificate information back to the factory defaults. Any existing certificates or private keys are deleted.

- **Delete Strong Authentication for Admin** – Removes strong authentication for the admin user login to allow you to use the console password.

Misc Menu

The **Misc** menu contains these options:

- **Set Time and Date** – Sets the time and date for the system.
- **Set Time Zone** – Sets your local time zone settings.
- **Configure UPS** – Allows you to configure the link to an Uninterruptible Power Supply (UPS) for automatic shutdown in the event of a power failure. A UPS keeps a device running for several minutes after a power outage. This allows you to shut down the device gracefully. The signal is sent with the serial COM port on the WatchGuard XCS that is connected to the UPS.
- **UPS Protocol** – Select the protocol to communicate with the UPS.

> ***Note*** *The system only supports APC type UPS systems.*

- **Enable UPS Monitor** – Select **Yes** to enable the UPS monitor.

  When you enable monitoring, the WatchGuard XCS detects alarms from the UPS that it is running on battery power, and starts a graceful shutdown of the WatchGuard XCS. If this option is set to **No**, the system does not automatically shut down, and you must perform a manual shut down before the UPS battery power is exhausted.

- **UPS Interface Port** – Select the serial COM port on the WatchGuard XCS that is connected to the UPS.
- **Shutdown Interval** – Type the number of minutes (0-30) to wait before automatically shutting down the WatchGuard XCS.
- **Configure Web Admin** – Modify the ports used to access the system web browser administration interface.
- **Configure Serial Console** – Allows you to configure a serial port for using the device console with a serial connection. To use the serial console, you must set your terminal program to these values:
  - VT100 Emulation
  - Baud Rate: 9600
  - Data Bits: 8
  - Parity: None
  - Stop Bits: 1
  - Flow Control: Hardware

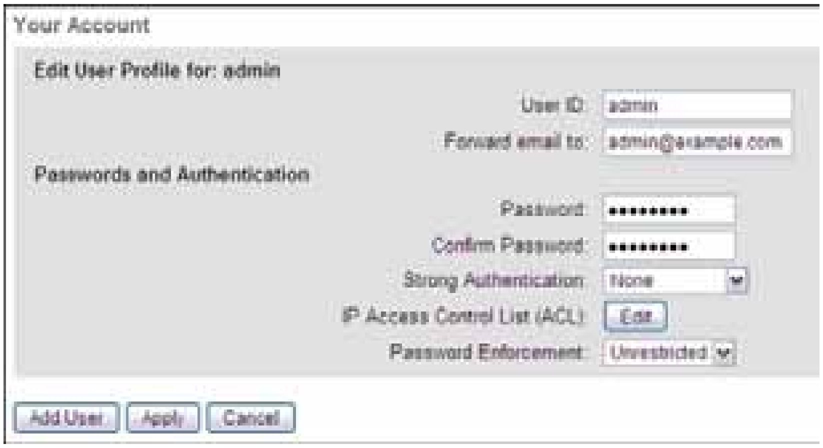
Configure the Admin User

The WatchGuard XCS creates the primary admin account during the initial installation. To modify the password or strong authentication settings for the admin user:

1. Select **Administration > Accounts > Administrator**.
2. In the **User ID** text box, you can view and modify the current admin user name.

   You cannot delete the admin user name, but you can modify the account name. This helps prevent attempts to compromise the primary admin user name by allowing you to use a non-standard user name. We recommended that you create additional admin users and use those accounts to manage the WatchGuard XCS instead of the primary admin account. Record the primary admin account password and store it in a safe place.

3. In the **Forward email to:** text box, type an optional email address to which to forward mail from this account.



Your Account

Edit User Profile for: admin

User ID: admin

Forward email to: admin@example.com

Passwords and Authentication

Password: •••••••••

Confirm Password: •••••••••

Strong Authentication: None

IP Access Control List (ACL): Edit

Password Enforcement: Unrestricted

4. In the **Password** text box, type and confirm a password for the admin user.
5. From the **Strong Authentication** drop-down list, you can configure optional strong authentication methods for the admin user.

   These methods of authentication require a hardware token that provides a response to the login challenge:

   - CRYPTOCard
   - SafeWord
   - SecurID

   A configuration wizard guides you through the steps to configure the token for the specified authentication method. See *Strong Authentication* for more detailed information.

4. In the **IP Access Control List (ACL)** section, click **Edit** to type a list of IP addresses or networks that are allowed admin access to this WatchGuard XCS.

   - Type a specific IP address, for example, `192.168.1.250`. To type a network address, use `192.168.1.0` for the entire 192.168.1.0/24 network.
   - Click **Add**.
   - You must also enable Admin access on a network interface (from **Configuration > Network >Interfaces**), in addition to the ACL access. Leave the IP access list undefined to limit admin access only through the network interface option.

4. From the **Password Enforcement** drop-down list, select a method to strengthen the security of the admin and user accounts.

   - **Unrestricted** – Allow any type of password for the admin account and user accounts. This is the default setting used after the initial installation.
   - **Strong** – Require that passwords for both admin accounts and user accounts be at least 6 characters in length and include a mix of alphabetic and non-alphabetic characters.

> ***Note*** *After you enable this option, any existing user accounts and passwords that do not have a strong password do not have the restrictions enforced until the next time you modify the passwords.*

Add Admin Users

There is only one primary admin user account, but you can add additional administrative users with *Tiered Administration*. This feature allows you to configure another user with full admin rights or with granular permissions that only give administrative rights to certain options.

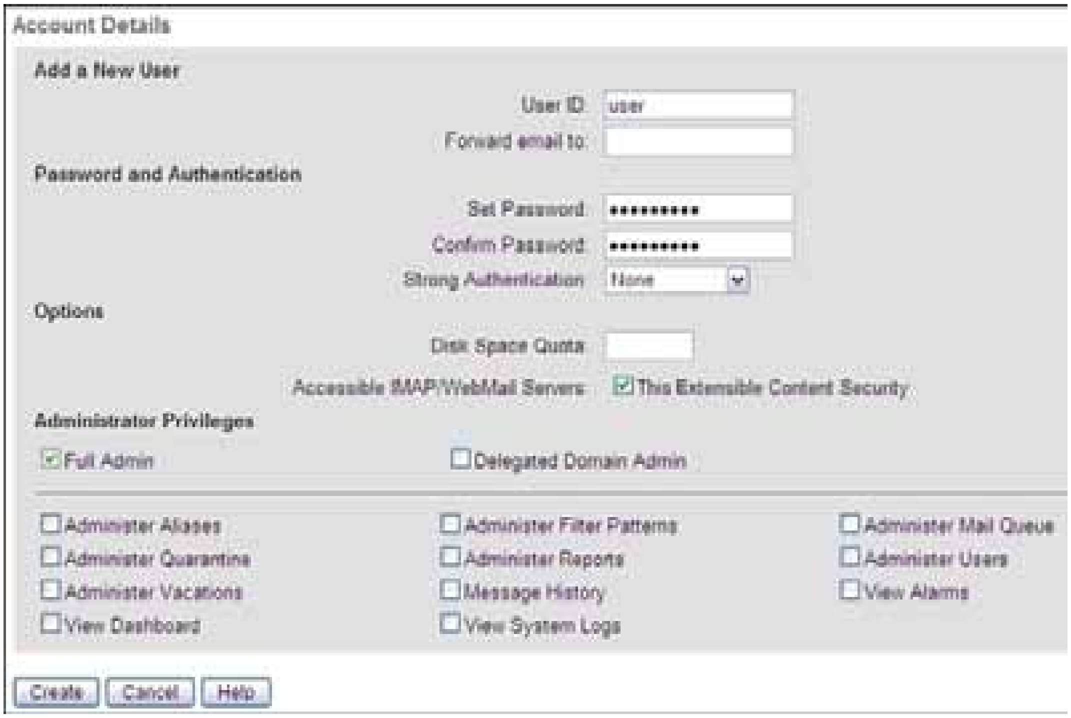
For example, you can add a user who has permissions to administer reports or vacation notifications, but does not have any other administrative access.

Granting full or partial admin access to one or more user accounts allows you to log actions performed by administrators because they have an identifiable user ID that can be tracked by the system.

> **Note** *A user with Full Admin privileges cannot modify the profile of the default admin user. They can, however, edit others users with Full Admin privileges.*

To add an administrative user:

1. Select **Administration > Accounts > Local Accounts**.
2. Click **Add Admin User**.



Account Details

Add a New User

User ID: user

Forward email to:

Password and Authentication

Set Password: ••••••••••

Confirm Password: ••••••••••

Strong Authentication: None

Options

Disk Space Quota:

Accessible IMAP/WebMail Servers: ☑ This Extensible Content Security

Administrator Privileges

☑ Full Admin ☐ Delegated Domain Admin

☐ Administer Aliases ☐ Administer Filter Patterns ☐ Administer Mail Queue

☐ Administer Quarantine ☐ Administer Reports ☐ Administer Users

☐ Administer Vacations ☐ Message History ☐ View Alarms

☐ View Dashboard ☐ View System Logs

3. In the **User ID** text box, type a user name.
4. In the **Forward email to:** text box, type an optional email address to which to forward messages from this account.
5. In the **Password** text box, type and confirm a password for this user.
6. From the **Strong Authentication** drop-down list, select an optional strong authentication method.
7. In the **Administrator Privileges** section, select the required administrative access for the user:

   Full Admin

The user has administrative privileges equivalent to the admin user.

Delegated Domain Admin

The user has administrative privileges to a specific domain. No tiered admin permissions are available when this is enabled.

Administer Aliases

The user can add, edit, remove, upload, and download aliases (except for LDAP aliases.)

Administer Filter Patterns

The user can add, edit, remove, upload, and download Pattern Filters and Specific Access Patterns.

Administer Mail Queue

The user can administer mail queues.

Administer Quarantine

The user can view, delete, and release quarantined files.

Administer Reports

The user can view, configure, and generate reports, and view system activity.

Administer Users

The user can add, edit, and relocate user mailboxes (except the Full Admin users). This includes the ability to upload and download user lists. The user can also configure User vacation notifications.

Administer Vacations

The user can edit local user's vacation notification settings and other global vacation parameters.

Message History

The user can view the message history database and perform quick searches of the recent Mail and Web activity on the Dashboard.

View Dashboard

The user can view the Dashboard page. Tiered admins can only perform a quick search of the recent mail and web activity if **Message History** is also enabled.

View Alarms

The user can view the alarms in the alarms indicator and the local alarms page, but cannot acknowledge them.

View System Logs

The user can view all system logs.

8. Click **Create**.
9. Select **Configuration > Network > Interfaces**.
10. Select the **Admin & Web User Login** and **WebMail** check boxes for the network interface to be used by tiered administration users.

See *Tiered Administration* for more information on configuring tiered admin access.

Admin User Automatic Logout and Lockout

As a security precaution, the WatchGuard XCS automatically logs the admin user out of the Web UI if they are logged in for 30 minutes without any activity.

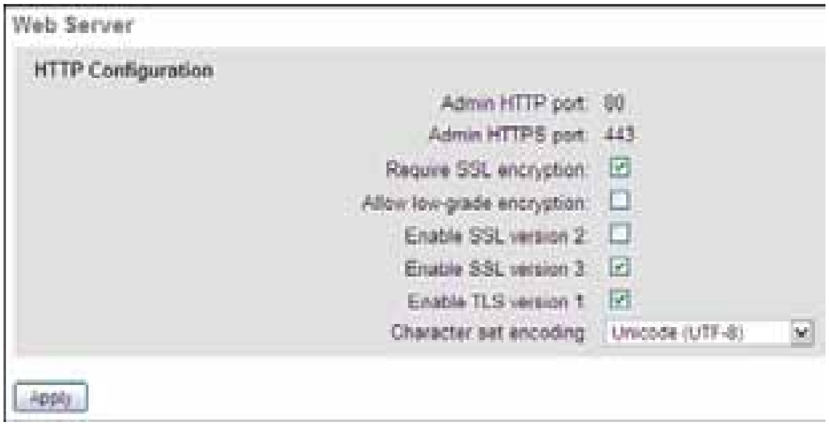
If login credentials for an admin user are not properly entered after five times in a row, the account is locked out for 30 minutes. Reboot the device to reset the lockout.

Web Server

The *Web Server* page defines the settings used to connect to the WatchGuard XCS with the Web UI. By default, the web server uses TCP port 80 for HTTP requests and TCP port 443 for HTTPS requests. For secure WebMail and administration sessions, we recommend that you leave the default SSL encryption enabled to force a connecting web browser to use HTTPS.

To configure your web server settings:

1. Select **Configuration > Network > Web Server**.



Web Server

HTTP Configuration

Admin HTTP port: 80

Admin HTTPS port: 443

Require SSL encryption: ☑

Allow low-grade encryption: □

Enable SSL version 2: □

Enable SSL version 3: ☑

Enable TLS version 1: ☑

Character set encoding: Unicode (UTF-8)

You can configure these options:

Admin HTTP Port

Indicates the default port 80 for HTTP requests.

Admin HTTPS Port

Indicates the default port 443 for HTTPS requests.

> ***Note*** *You can only modify the HTTP/HTTPS ports on the WatchGuard XCS console.*

Require SSL encryption

Requires SSL encryption for all user and administrator web sessions.

Allow low-grade encryption

Allow the use of low-grade encryption, for example, DES ciphers with a key length of 64 bits, for encrypted user and administrator web sessions.

Enable SSL version 2

Enables SSL version 2 protocol. Note that SSL version 2 contains known security vulnerabilities.

Enable SSL version 3

Enable SSL version 3 protocol. This is the default setting.

Enable TLS version 1

Enable TLS version 1 protocol. This is the default setting.

Character set encoding

Select the type of character encoding used to display HTML data. Change the encoding if you view and manage dictionaries that use different encodings, for example, ISO-8859-1.

2. Click **Apply**.

External Proxy Server

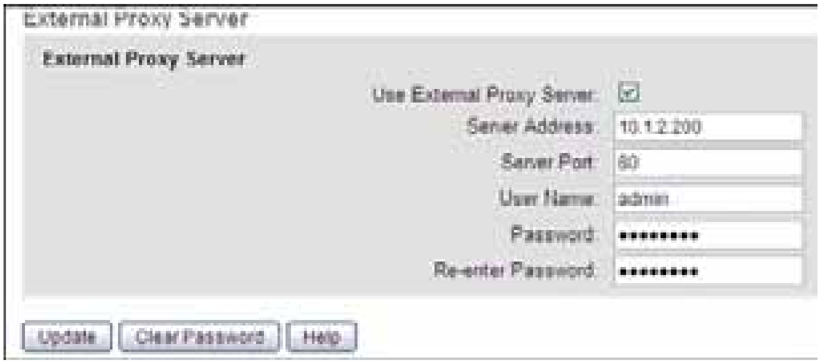
A proxy server is used to cache and proxy requests to systems external to your network. If you use features that must connect to the Internet for updates, and your network uses a proxy server, the proxy server must be configured on the WatchGuard XCS. If you do not use an external proxy server, keep this option disabled.

The WatchGuard XCS requires access to the Internet through the proxy server for these features:

- Kaspersky and McAfee Anti-Virus pattern updates
- Message encryption with a public key server
- Reputation Enabled Defense sharing uploads
- URL Categorization control list downloads
- Security Connection features and software
- Intercept Anti-Spam database and Brightmail updates
- SecureMail encryption connection
- Feature key updates

To configure an external proxy server:

1. Select **Configuration > Network > External Proxy Server**.



External Proxy Server

External Proxy Server

Use External Proxy Server: ☑

Server Address: 10.1.2.200

Server Port: 80

User Name: admin

Password: •••••••••

Re-enter Password: •••••••••

2. Select the **Use External Proxy Server** check box.
3. In the **Server Address** text box, type the IP address or host name of the proxy server.
4. In the **Server Port** text box, type the **Server Port** number used by the proxy server.
5. In the **User Name** text box, type a user name used to log in to the proxy server if authentication is required.
6. Type and confirm a **Password** for the user name on the proxy server.
7. Click **Update**.

Customize the Web UI Interface

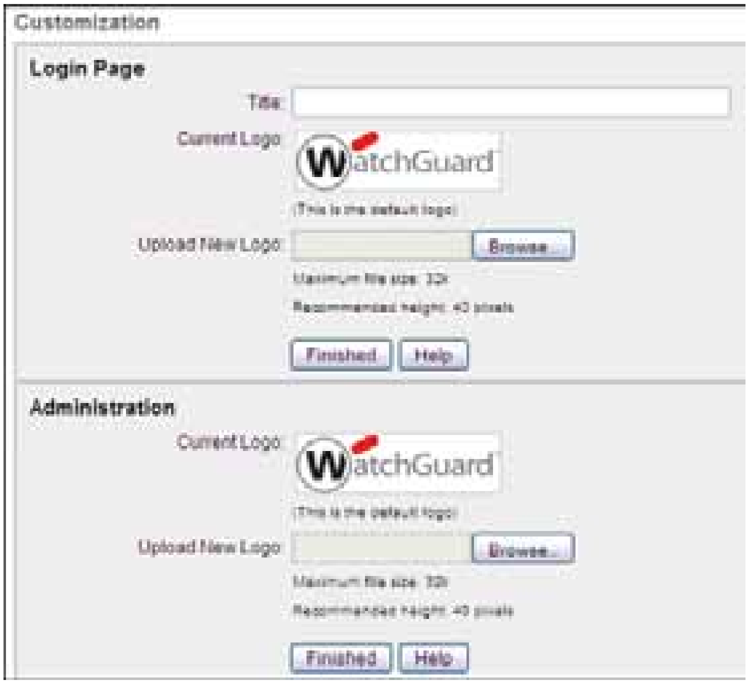
The WatchGuard XCS interface logos can be easily customized. You can replace the system logo with your own custom logo.

You can modify these logos:

- Login page logo
- Administration page logo (also appears on generated reports)
- Spam digest logo

To customize a logo:

1. Select **Configuration > Miscellaneous > Customization**.



Customization

Login Page

Title:

Current Logo:

(This is the default logo)

Upload New Logo:

Maximum file size: 32k

Recommended height: 40 pixels

Administration

Current Logo:

(This is the default logo)

Upload New Logo:

Maximum file size: 32k

Recommended height: 40 pixels

2. In the **Title** text box, type optional text for the title bar of the login page.
3. For the logo you want to customize, click **Browse** to choose a file, and then click **Next** to upload the file.

   Most graphic formats are supported (GIF, JPEG, PNG, BMP), but we recommend that you use graphics suitable for web pages, for example, GIF and JPEG. The maximum file size is 32k with a recommended height of 40 pixels.

   Select the **Reset this Logo to the Default** link to revert to the default logo.

4. Click **Finished**.

Customize the HTTP Proxy End-User Agreement

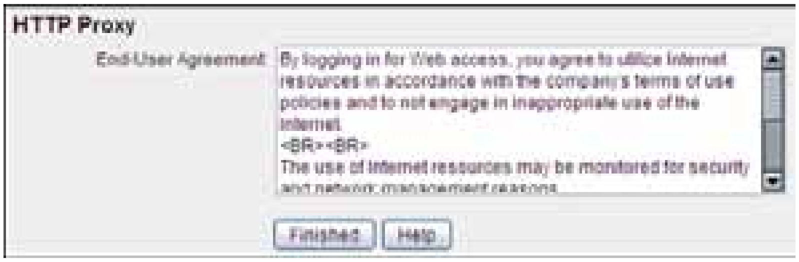
You can customize the *HTTP Proxy End-User Agreement* text that appears to users when they log in through the Web Portal. The Web Portal login page appears to end users when **IP Address Portal Authentication** is enabled as the authentication method in the HTTP Proxy configuration.

The user must accept this agreement and successfully authenticate before they are allowed to browse the web through the Web Proxy.

> ***Note*** *The logo that appears on the Web Portal page is the Administration page logo.*

To customize the agreement:

1. Select **Configuration > Miscellaneous > Customization**.



End-User Agreement: By logging in for Web access, you agree to utilize Internet resources in accordance with the company's terms of use policies and to not engage in inappropriate use of the Internet.
<BR><BR>
The use of Internet resources may be monitored for security and network management reasons

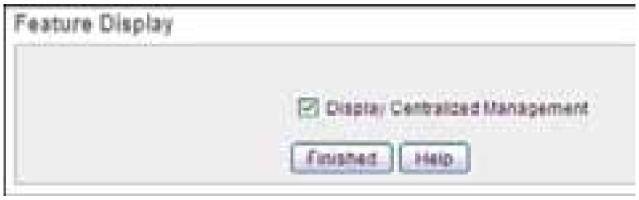
2. In the **End-User Agreement** text box, customize the **End-User Agreement** text as required.
3. Click **Finished**.

Feature Display

You can choose to display or hide specific feature configuration entries in the main menu, the Dashboard, and policy configuration.

For example, if you do not use the Centralized Management feature, you can prevent any Centralized Management options from appearing in the menus.

1. To configure feature display:
2. Select **Configuration > Miscellaneous > Feature Display**.



☑ Display Centralized Management

3. Select the **Display Centralized Management** check box to show configuration options for this feature in the menu.

   Clear the check box to prevent the display of any Centralized Management options.

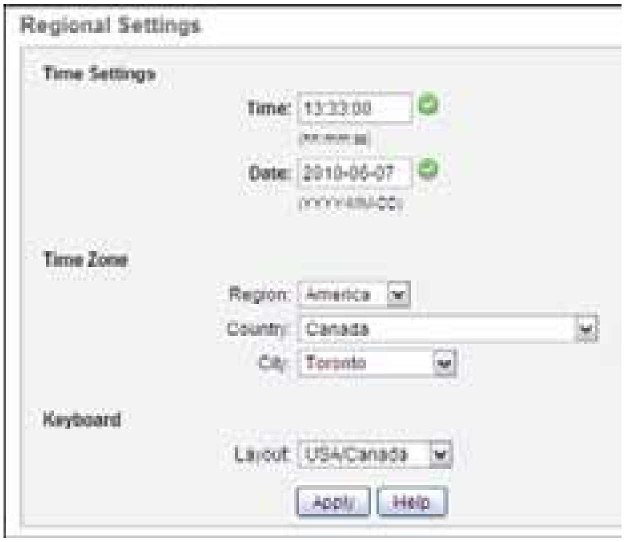
4. Click **Finished**.

Regional Settings

Your regional settings (time and date, time zone, and keyboard layout settings) are configured during the initial installation process.

To modify your regional settings:

1. Select **Administration > System > Regional Settings**.



Regional Settings

Time Settings

Time: 13:33:00 (hh:mm:ss)

Date: 2010-06-07 (YYYY-MM-DD)

Time Zone

Region: America

Country: Canada

City: Toronto

Keyboard

Layout: USA/Canada

2. In the **Time Settings** section, set the current date and time.
   - In the **Time** text box, type the current time. Use 24-hour format HH:MM:SS.
   - In the **Date** text box, type the current date. Use the format YYYY-MM-DD.

> ***Note*** *You can configure an NTP Time Server in the Network Settings to make sure the system time is always synchronized.*

3. In the **Time Zone** section, from the **Region**, **Country**, and **City** drop-down lists, select the closest city to your location and time zone.
4. In the **Keyboard** section, from the **Layout** drop-down list, select the keyboard layout for your location.
   The keyboard is used to access the system console.

6 Configure Mail Delivery

Network Configuration

When you complete the initial installation process for your WatchGuard XCS, you configure the basic network information for your device. From the **Network Configuration** page, you can configure other network interfaces and advanced network settings.

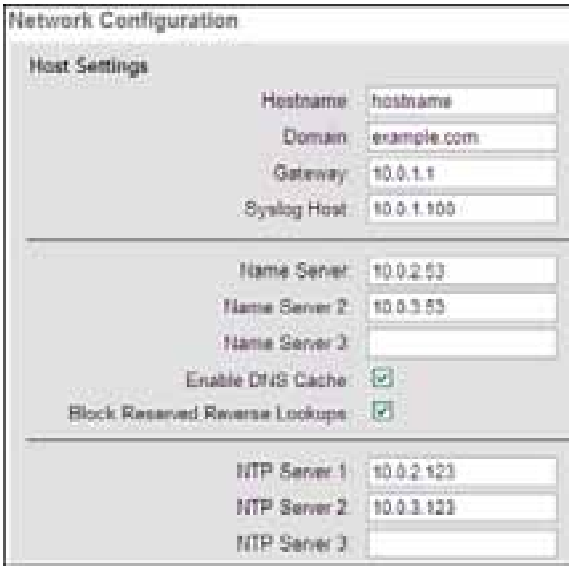
You can modify these configuration items:

- Hostname and Domain information
- Default Gateway
- Syslog Host
- DNS and NTP servers
- Network interface IP Address and feature access settings
- Clustering and Queue Replication interface configuration
- Web Proxy Bridging and Transparent Mode
- Support Access settings

> ***Note*** *If you make any modifications to your network settings, you must reboot the system. The system prompts you to restart after you apply the configuration.*

To configure your network settings:

1. Select **Configuration > Network > Interfaces**.
   The Network Configuration page appears.



Network Configuration

Host Settings

Hostname	hostname
Domain	example.com
Gateway	10.0.1.1
Syslog Host	10.0.1.100
Name Server	10.0.2.53
Name Server 2	10.0.3.53
Name Server 3	
Enable DNS Cache	☑
Block Reserved Reverse Lookups	☑
NTP Server 1	10.0.2.123
NTP Server 2	10.0.3.123
NTP Server 3	

2. The **Hostname**, **Domain**, and **Gateway** are configured during the initial installation and can be modified on this page.
3. In the **Hostname** text box, type the hostname (not the Fully Qualified Domain Name) of this device.

   For example, if your Fully Qualified Domain Name is hostname.example.com, type `hostname`.
4. In the **Domain** text box, type the domain name for your device.

   For this example, type `example.com`.
5. In the **Gateway** text box, type the IP address of the default route for this device.
   This is usually the external router connected to the Internet or the network firewall's interface if the system is located on the DMZ network.
6. If you use a syslog host on your network, in the **Syslog Host** text box, type the IP address or hostname of your syslog host.
   A syslog host collects and stores log files from many sources.
7. In the **Name Servers** text boxes, type the name of your primary and secondary DNS servers.
   At least one DNS (Domain Name Service) name server must be configured for hostname resolution. We recommend that you specify at least one secondary DNS server to use when the primary DNS server is unavailable.
8. To enable DNS caching, select the **Enable DNS Cache** check box.

   This option is enabled by default and provides the best performance in most cases. When this option is enabled, the system determines which of the configured DNS servers sends the fastest response, and caches the result.

   Clear the **Enable DNS Cache** check box to:
9. Use the configured DNS servers in the order they appear
10. Use your ISP DNS servers as failover servers
11. To make sure private reserved IP addresses are not used in a reverse lookup to a DNS server, select the **Block Reserved Reverse Lookups** check box.

    This option is enabled by default.

Clear the **Block Reserved Reverse Lookups** check box if you use your ISP DNS servers, and reverse lookups for reserved addresses are required in your network environment.

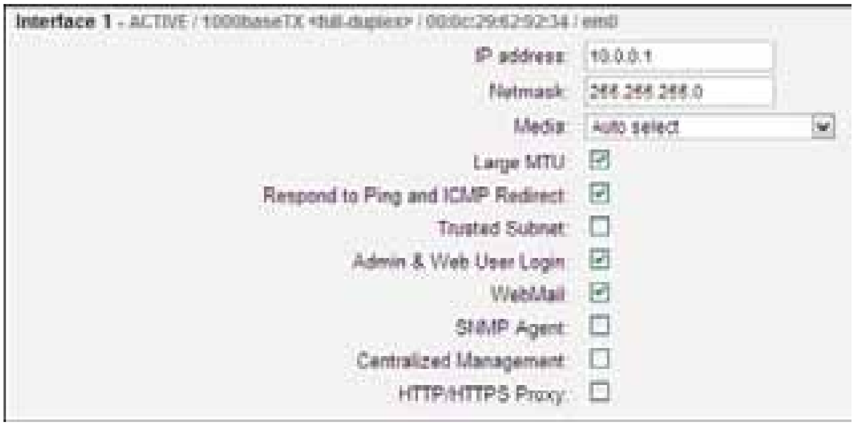
12. In the **NTP Server** text boxes, type the IP address or hostname for your primary time server and any secondary time servers.
    We recommend that you specify secondary NTP servers to use if the primary NTP server is unavailable.

Network Interface Configuration

For each network interface, you can set these options:

1. Type an **IP Address** for this interface.

   For example, `10.0.0.1`.



Interface 1 - ACTIVE / 1000baseTX <full-duplex> / 00:0c:29:62:92:34 / em0

IP address: 10.0.0.1

Netmask: 255.255.255.0

Media: Auto select

Large MTU: ☑

Respond to Ping and ICMP Redirect: ☑

Trusted Subnet: □

Admin & Web User Login: ☑

WebMail: ☑

SNMP Agent: □

Centralized Management: □

HTTP/HTTPS Proxy: □

2. Type the **Netmask** for this interface.

   For example, `255.255.255.0`.

3. Select the **Media** type for the network card.
   For automatic configuration, select Auto select.

4. There are several additional options that you can enable on a network interface.
   Some of the following options will not be displayed unless the related feature is enabled.

   Large MTU

   > Sets the MTU (Maximum Transfer Unit) to 1500 bytes. The regular MTU size is 576 bytes. Large MTU can improve performance connecting to servers on the local network. You must enable Large MTU if you are using the Web Proxy. This option is enabled by default, and should only be disabled if required and in consultation with a Technical Support representative.

   Respond to Ping and ICMP Redirect

   > Allows ICMP ping requests to this interface. This allows you to perform network connectivity tests to this interface, but makes this interface more susceptible to denial of service ping attacks.

   Trusted Subnet

Consider all hosts on this subnet trusted for mail relaying, and exclude them from Anti-Spam processing.

Admin and Web Login

Allows access to this interface for administrative purposes. This includes Tiered Admin users and Web users.

WebMail

Allows access to WebMail through this interface. This includes the WebMail client, Secure WebMail, Tiered Admin, User Spam Quarantine, and Trusted/Blocked Senders List access.

IMAPS Server

Allows secure access to the internal IMAP server through this interface.

IMAP Server

Allows access to the internal IMAP server through this interface.

POP3S Server

Allows secure access to the internal POP3 server through this interface.

POP3 Server

Allows access to the internal POP3 server through this interface.

SNMP Agent

Allows access to the SNMP (Simple Network Management Protocol) agent through this network interface. You should only enable access to the SNMP agent on an internal interface.

Centralized Management

Enables Centralized Management on this interface.

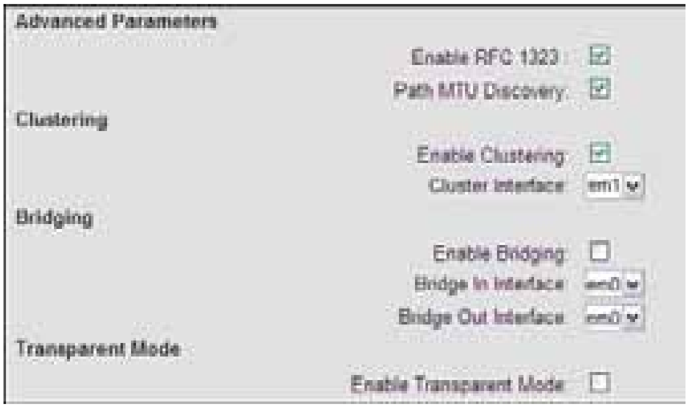
HTTP/HTTPS Proxy

Enables access to the HTTP proxy on this interface.

5. Click **Apply**.
   You must restart the device.

Advanced Parameters

These advanced networking parameters are TCP extensions that improve the performance and reliability of communications.



Advanced Parameters

Enable RFC 1323: ☑
Path MTU Discovery: ☑

Clustering

Enable Clustering: ☑
Cluster Interface: em1

Bridging

Enable Bridging: □
Bridge In Interface: em0
Bridge Out Interface: em0

Transparent Mode

Enable Transparent Mode: □

Enable RFC 1323

Enable RFC 1323 TCP extensions to improve performance and to provide reliable operations of high-speed paths. This option is enabled by default. Disable this option if you experience networking issues with certain hosts.

Path MTU Discovery (RFC 1191)

Path MTU is enabled by default. Disable Path MTU (Maximum Transfer Unit) to resolve delivery problems when interconnecting between specific firewalls and SMTP proxies.

Clustering

Use the options in the Clustering section to configure clustering on a specific network interface.
See *Configure Clustering* for more detailed information on clustering.

To enable clustering:

1. Select **Configuration > Network > Interfaces**.
2. Go to the **Clustering** section.
3. Select the **Enable Clustering** check box.
4. From the **Cluster Interface** drop-down list, select the interface to connect to the cluster network.
5. Click **Apply**.
   You must restart the system.

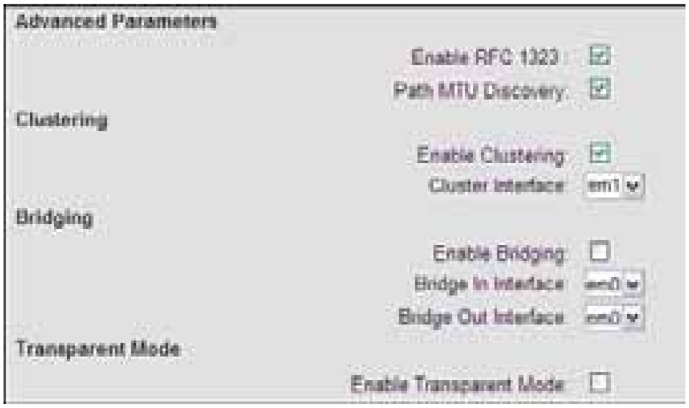
Transparent Mode and Bridging

The Web Proxy feature offers a Transparent Mode to integrate the Web Proxy more easily into existing environments with minimal network configuration. In a typical Transparent Mode implementation, the Web Proxy system sits inline between the primary internal switch or router and an existing network firewall. This enables the Web Proxy to act as a bridge for all non-local traffic, except selected HTTP traffic that is proxied. Packet inspection is performed on all traffic to determine if data is proxied or bridged.

See *Transparent Mode* for more detailed information.

To configure Transparent Mode bridging for the Web Proxy:

1. Select **Configuration > Network > Interfaces**.
2. Go to the **Bridging** and **Transparent Mode** sections.



Advanced Parameters

Enable RFC 1323: ☑

Path MTU Discovery: ☑

Clustering

Enable Clustering: ☑

Cluster Interface: em1

Bridging

Enable Bridging: □

Bridge In Interface: em0

Bridge Out Interface: em0

Transparent Mode

Enable Transparent Mode: □

3. Select the **Enable Bridging** check box.

   This option is required for Transparent Web Proxy mode. When you enable bridging, you must select two network interfaces for the bridge.

4. Select a network interface to use as the **Bridge In Interface** in Transparent Mode.

   For greater security and performance, make sure this interface is on a dedicated, non-routable subnet. You must assign an IP address and select the **HTTP/HTTPS Proxy access** and **Large MTU** check boxes before you select the interface as the Bridge In interface. This IP address is used as the address for the entire bridge interface.

5. Select a network interface to use as the **Bridge Out Interface** in Transparent Mode.

   For greater security and performance, make sure this interface is on a dedicated, non-routable subnet. This interface does not require an IP address and is configured automatically for use with the bridge.

6. Select the **Enable Transparent Mode** check box.
7. Click **Apply**.
   You must restart the system.

Support Access

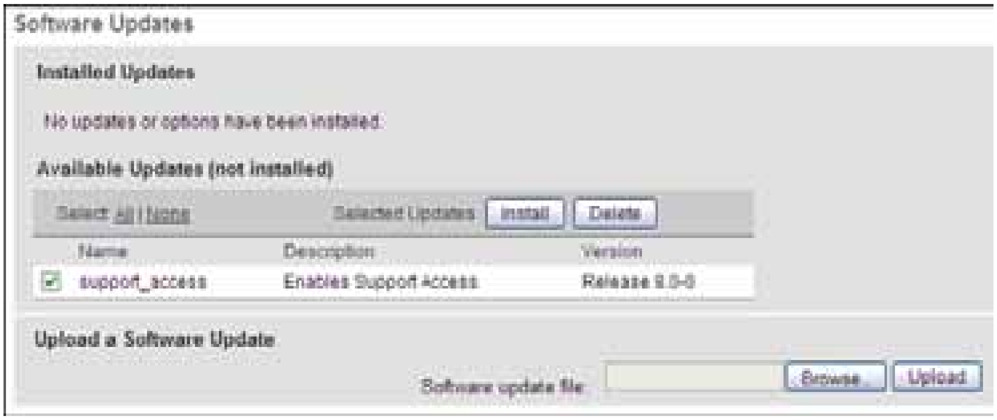
Support Access enables technical support to connect to this system from the specified IP address. This setting is usually not enabled during normal use, and should only be enabled if requested by technical support.

For security reasons, Support Access communications use SSH (Secure Shell) to establish a secure connection based on PKI (Public Key Infrastructure) encryption on a non-standard network port. Support Access only allows a connection from WatchGuard networks.

> **Note** *You must open up TCP port 10101 on your firewall to enable support access to work behind a network firewall.*

To install and enable Support Access:

1. Select **Administration > Software Updates > Updates**.



Software Updates

Installed Updates

No updates or options have been installed.

Available Updates (not installed)

Select: All | None — Selected Updates: Install Delete

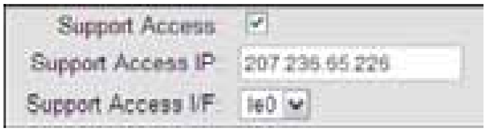
	Name	Description	Version
☑	support_access	Enables Support Access	Release 9.0-0

Upload a Software Update

Software update file: Browse... Upload

2. Select the **support_access** update check box.
3. Click **Install**.

   The system reboots.
4. Select **Configuration > Network > Interfaces**.
5. Go to the **Support Access** section.



Support Access ☑

Support Access IP: 207.236.65.226

Support Access I/F: le0

6. To enable Support Access on this system, select the **Support Access** check box.

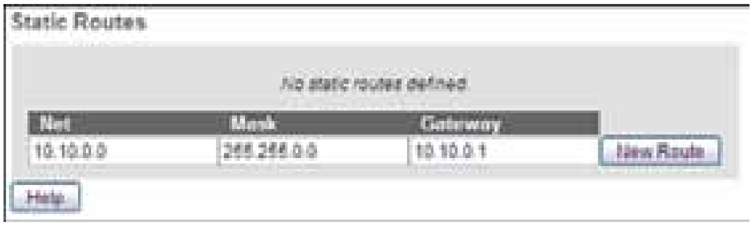
   Support access is allowed to originate from the specified Support Access IP Address.
7. From the **Support Access I/F** drop-down list, select the network interface for which you want to enable Support Access.
8. Click **Apply**.

Static Routes

Static routes are required if the messaging servers to which messages must be relayed are located on another network, for example, behind an internal router, firewall, or accessed through a VPN.

To add a static route:

1. Select **Configuration > Network > Static Routes**.



Static Routes

No static routes defined.

Net	Mask	Gateway	
10.10.0.0	255.255.0.0	10.10.0.1	New Route

Help

2. In the **Net** text box, type a network address.

   For example, `10.10.0.0`.
3. In the **Mask** text box, type a corresponding net mask.

   For example, `255.255.0.0`.

4. In the **Gateway** text box, type a gateway for the network.

   For example, `10.10.0.1`.

5. Click **New Route**.

Virtual Interfaces

Virtual Interfaces are additional interfaces and IP addresses used to send and receive mail for specific domains. These virtual interfaces are associated with the existing physical network interfaces on the WatchGuard XCS.

The system sends all outbound email for a specific domain using its specified IP address in the Virtual Interfaces configuration. The WatchGuard XCS selects the virtual interface to use for outgoing mail by matching the sender's domain to the domains associated with the configured virtual interfaces. If no virtual interface domains match the domain of the sender, or if using the virtual interface results in a non-network connection, the system sends the mail through its normal outbound interface.

The WatchGuard XCS accepts inbound email arriving through this virtual interface's IP address. When a mail server connects to SMTP port 25 on a virtual interface, the customized banner for that interface appears. If no banner is specified, the default system banner is used. To configure the banner, select **Configuration > Mail > Access**.

Only TCP port 25 is used for sending and receiving mail on a virtual interface. Virtual interfaces can be pinged if ping is enabled on the corresponding physical network interface. Because of their nature, virtual interfaces cannot be pinged from the **Utilities** page, and cannot be used when the Web Proxy is in Transparent Mode. You can only configure virtual interfaces on up to five different physical network interfaces.

Domains that use virtual interfaces are used with Domain-based policies to provide flexibility in creating security and content policies for specific domains.

The WatchGuard XCS supports up to 175 Virtual Interfaces. This feature does not currently support IDN (Internationalized Domain Names).

Network routing of virtual interfaces

Virtual interfaces are routed through:

- A physical interface that shares the same subnet as the Virtual Interface.
- The physical interface that reaches a host specified through a static route.
- The current default route (through the physical interface that connects to the default router.)

If your system has these settings:

- Interface 1: 192.168.1.10/24
- Interface 2: 172.16.1.10/16
- Default Gateway/Router: 172.16.1.1

Adding a virtual interface of 192.168.1.20 routes through Interface 1.

Adding a virtual interface of 172.16.1.20 routes through Interface 2.

Adding a virtual interface of 10.10.1.20 routes through Interface 2 through the default gateway.

If the virtual interface has no corresponding physical interface displayed, there is no valid route through any physical interface, and the virtual interface is disabled.

To configure virtual interfaces:

1. Select **Configuration > Network > Virtual Interfaces**.
2. Upload a virtual interface list in CSV format that contains comma or tab separated entries.

   Use this format:

   ```
   [domain],[IP Address],[Banner message]
   ```

   For example,

   ```
   example1.com,10.2.45.10,example1.com ESMTP
   ```

> ***Note*** *A standards-compliant banner should, at minimum, contain the domain name and the keyword ESMTP, for example, "example.com ESMTP". Extra informational text after the ESMTP keyword is optional, for example, "example.com ESMTP Authorized Users Only".*

You must use a text editor to create the file vip.csv.

To update a virtual interface file:

1. To download the virtual interface list from the WatchGuard XCS, click **Download File**.
2. Open the file and update the virtual interface list.
3. Click **Upload File** and upload the edited file to the WatchGuard XCS.
4. For each domain that to be used with Virtual Interfaces, select **Configuration > Mail > Routing** to define a mail route to a destination mail server.
   Virtual mappings can also be used for mail routing.

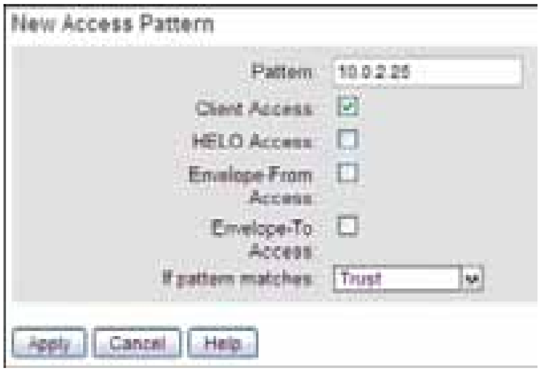
You must publish DNS MX records for any virtual interfaces. You must also configure local network devices, for example, the default external router to route traffic to and from the virtual interfaces.

Virtual Interfaces and Trusts

Email arriving through a virtual interface is considered untrusted for Anti-Spam and security processing. To configure a client as trusted, use a Specific Access Pattern or Pattern Filter to trust the client that connects on that virtual interface.

To trust a client with a Specific Access Pattern:

1. Select **Configuration > Mail > Access**.
2. Click the **Add Pattern** button.



New Access Pattern

Pattern	10.0.2.25
Client Access	☑
HELO Access	□
Envelope-From Access	□
Envelope-To Access	□
If pattern matches	Trust

3. In the **Pattern** field, type the IP address of the client.
4. Select the **Client Access** check box.
5. From the **If pattern matches** drop-down list, select **Trust**.
6. Click **Apply**.

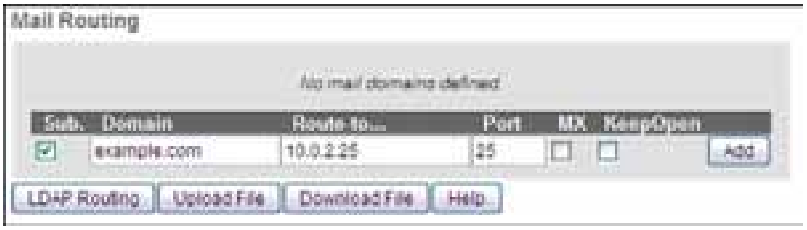
Mail Routing

If you configured a primary email domain and an internal mail server during the initial installation of the WatchGuard XCS, a mail route is automatically set up for that mail server.

Use the *Mail Routing* page to configure additional domains to accept mail for and identify the destination mail servers to route the messages to.

To add and configure mail routes:

1. Select **Configuration > Mail > Routing**.



Mail Routing

No mail domains defined

Sub.	Domain	Route to...	Port	MX	KeepOpen	
☑	example.com	10.0.2.25	25	□	□	Add

2. To accept and relay mail for subdomains of the specified domain, select the **Sub** option.
3. In the **Domain** text box, type the domain for which mail is accepted.

   For example, `example.com`.
4. In the **Route-to** text box, type the IP address for the mail server to which mail is delivered.

   For example, `10.0.2.25`.
5. In the **Port** text box, type the port on which to deliver mail to this server.
   The default is SMTP port 25.
6. If you need to look up the mail routes in DNS before delivery, select the **MX** option.

   If this option is disabled, MX records are ignored. You do not need to select this item unless you are using multiple mail server DNS entries for load balancing and failover purposes. By checking the MX record, DNS sends the request to the next mail server in the list.

7. Select the **KeepOpen** option to make sure that each mail message to the domain is not removed from the active queue until the WatchGuard XCS attempts delivery, even if the preceding mail failed or was deferred.
   This setting makes sure that local mail servers receive high priority.

   > ***Note*** *The KeepOpen option should only be used for domains that are usually very reliable. If the domain is unavailable, it can cause system performance problems because of excessive error conditions and deferred mail.*

8. Click **Add**.
9. Repeat the procedure for any additional domains and mail servers.

Upload Mail Routes

You can upload a list of mail routes in a text file. The file must contain comma or tab separated entries with one entry per line.

Use this format:

```
[domain],[route],[port],[ignore_mx],[subdomains_too],[keepopen]
```

For example:

```
example.com,10.0.2.25,25,on,off,off
```

You must use a text editor to create the file domains.csv.

To update a mail route file:

- To download the mail route list from the WatchGuard XCS, click **Download File**.
- Open the file and update the mail route list.
- Click **Upload File** and upload the edited file to the WatchGuard XCS.

Subdomain Routing with MX Lookup

The WatchGuard XCS can route and deliver messages to subdomains based upon an MX record lookup using the domain portion of the RCPT TO: field of a message.

In the Mail Routing configuration, you can specify “any” or “ANY” in the **Route-to** field. The WatchGuard XCS performs an MX lookup on the specified subdomain, and then the message is delivered based on a DNS A record lookup for the destination host.

When you define the **Route-to** field as “any” or “ANY”, these default values are used, and changing them in the user interface has no effect.

- The default **Port** is 25
- The **MX** option is enabled
- The **KeepOpen** option is disabled

Subdomain Routing and DNS Caching

If DNS caching is enabled, a cached DNS entry can cause a message to be delivered to an incorrect host if the DNS entry is modified. We recommend that you disable the **Enable DNS Cache** option (from **Configuration > Network > Interfaces**) if you use DNS MX lookups for subdomain routing. This can cause a slight decrease in performance of DNS lookups, but makes sure the correct route is used if you change a DNS record.

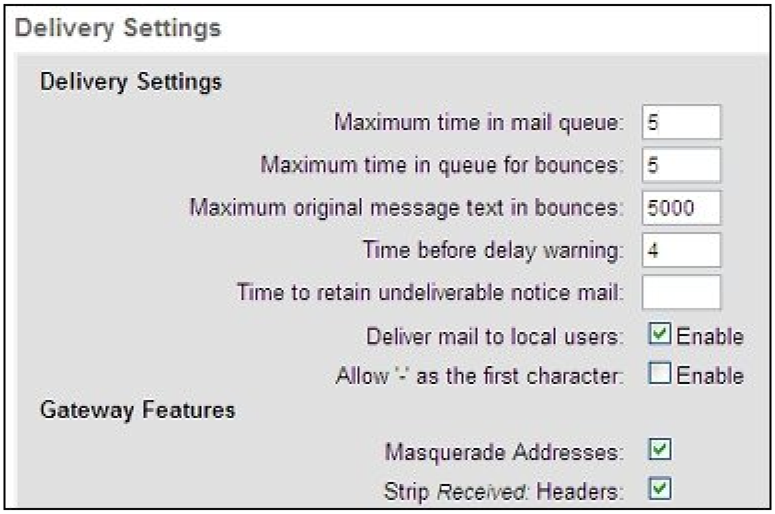
LDAP Routing

Click the **LDAP Routing** button to define mail routes using an LDAP directory server. This is the preferred mail routing method for organizations with a large amount of domains. See *LDAP Routing* for more detailed information on using LDAP for mail routing.

Mail Delivery Settings

Use the *Mail Delivery Settings* page to configure parameters related to accepting, relaying, and delivering mail messages.

To configure your mail delivery settings, select **Configuration > Mail > Delivery**.



Delivery Settings

Delivery Settings

Maximum time in mail queue: 5

Maximum time in queue for bounces: 5

Maximum original message text in bounces: 5000

Time before delay warning: 4

Time to retain undeliverable notice mail:

Deliver mail to local users: ☑ Enable

Allow '-' as the first character: □ Enable

Gateway Features

Masquerade Addresses: ☑

Strip *Received:* Headers: ☑

Delivery Settings

Maximum time in mail queue

Type the number of days for a message to stay in the queue before it is returned to the sender as “undeliverable”. The default is 5 days.

Maximum time in queue for bounces

Type the number of days a system-generated bounce message (from MAILER-DAEMON) is queued before it is considered undeliverable. Default is 5 days. Set this value to 0 to attempt delivery of bounce messages only once.

Maximum original message text in bounces

Type the maximum amount (in bytes) of original message text that is sent in a non-delivery notification. Range is 10 to 1000000000. If this field is left blank, the default is set to 5000 bytes.

Time before delay warning

Number of hours before issuing the sender a notification that mail is delayed. Set to “0” to disable this option. The default is 4 hours.

Time to retain undeliverable notice mail

The number of hours to keep undeliverable notice mail addressed to the external mail server’s MAILER-DAEMON. These messages are typically notifications sent to mail servers with invalid return addresses and can be safely purged. Leave this value blank for no special processing.

Deliver mail to local users

Disable this option to prevent mail delivery to local accounts configured on the WatchGuard XCS. The postmaster (admin) account is not affected by this setting.

Allow “-” as the first character

Allows a recipient address to have a “-” character as the first character in the address, for example, “-test@example.com”.

Gateway Features

Masquerade Addresses

Masquerades internal host names by rewriting headers to only include the address of this system.

Strip Received Headers

Strips all Received headers from outgoing messages.

Default Mail Relay

Relay To

(Optional) Type an optional hostname or IP address of a mail server (not this system) to which to relay mail for all email with unspecified destinations. A recipient’s email domain is checked against the mail routing table. If the destination is not specified, the email is sent to the Default Mail Relay server for delivery. You this option when the WatchGuard XCS cannot deliver email directly to remote mail servers. If you are setting up this system as a dedicated WebMail system, and all mail originating from this system should be forwarded to another mail server for delivery, then specify the destination mail server here.

> ***Warning*** *Do not enter the name of your system because this causes a relay loop.*

SMTP Port

Type the SMTP port used to deliver mail to the relay. The default is 25.

Ignore MX record

Enable this option to prevent an MX record lookup for this host to force relay settings.

Enable Client Authentication

Enable client SMTP authentication for relaying mail to another mail server. This option is only used in conjunction with the Default Mail Relay feature. This allows the WatchGuard XCS to authenticate to a server that it is using to relay mail. With this configuration, connections to the default mail relay are authenticated, while connections to other mail routes are not.

User ID

Type a User ID to login to the relay mail server.

Password

Type and confirm a password for the specified User ID.

Failback Mail Relay

Relay To

Enter an optional hostname or IP address of a mail server (not this system) to be used as the failback server. In the event the default mail relay is unavailable, the failback server relays mail for all email with unspecified destinations.

SMTP Port

Type the SMTP port to use to deliver mail to the relay. The default is 25.

Ignore MX record

Enable this option to prevent an MX record lookup for this host to force relay settings.

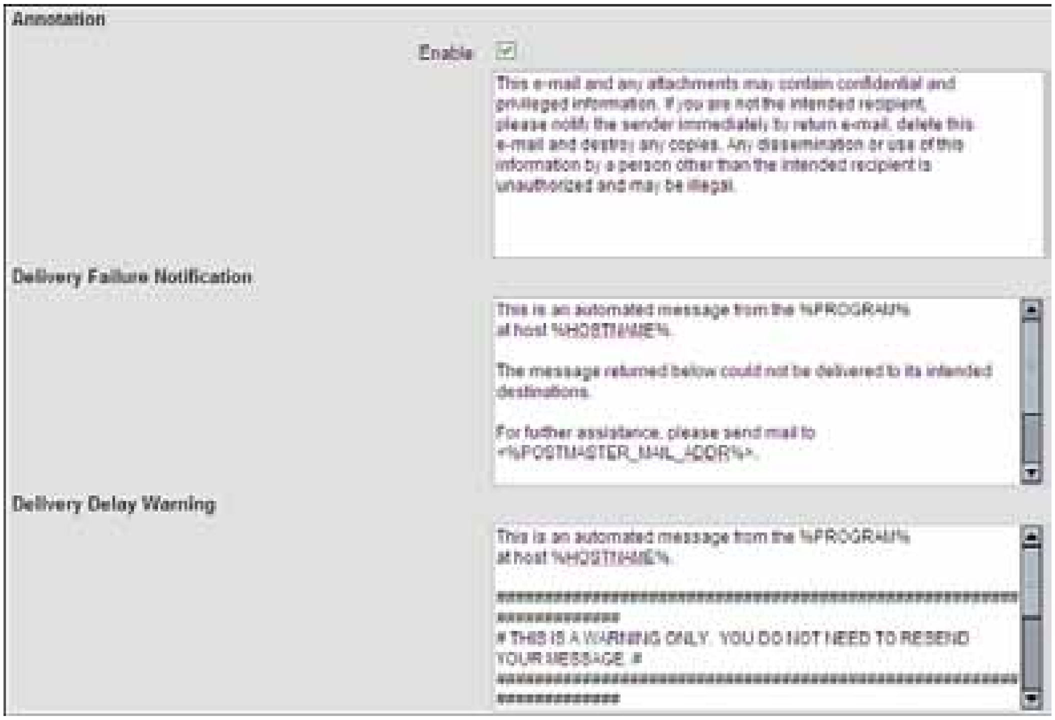
BCC (Blind carbon copy) All Mail

The WatchGuard XCS offers an archiving feature for organizations that require storage of all email that passes through their corporate mail servers. This option sends a blind carbon copy (BCC) of each message that passes through the system to the specified address. This address can be local or on any other system. Once copied, the mail can be effectively managed and archived from this account. You must also specify an address that receives error messages if there are problems delivering the BCC messages.

Annotations and Delivery Warnings

You can enable and customize *Annotations* that are appended to all messages, and customize *Delivery Failure* and *Delivery Delay* warning messages.

Note *Some mail clients display notifications and annotations as attachments to a message rather than in the message body.*



Annotation

Enable ☑

This e-mail and any attachments may contain confidential and privileged information. If you are not the intended recipient, please notify the sender immediately by return e-mail, delete this e-mail and destroy any copies. Any dissemination or use of this information by a person other than the intended recipient is unauthorized and may be illegal.

Delivery Failure Notification

This is an automated message from the %PROGRAM%
at host %HOSTNAME%.

The message returned below could not be delivered to its intended destinations.

For futher assistance, please send mail to
<%POSTMASTER_MAIL_ADDR%>.

Delivery Delay Warning

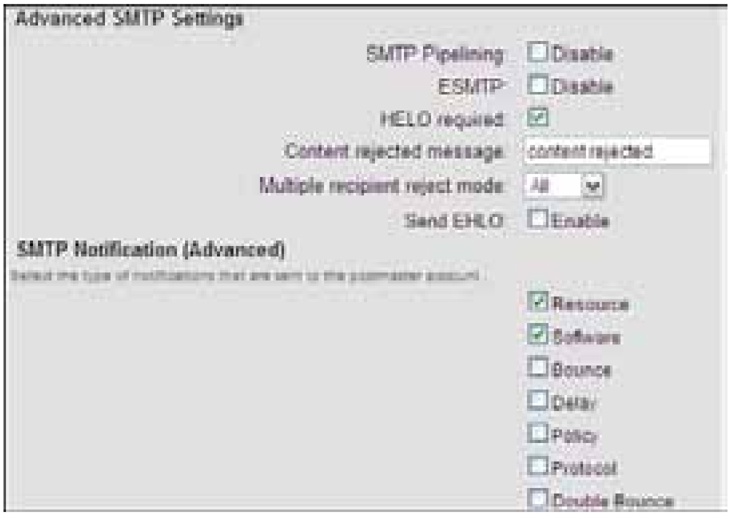
This is an automated message from the %PROGRAM%
at host %HOSTNAME%.

###
THIS IS A WARNING ONLY. YOU DO NOT NEED TO RESEND YOUR MESSAGE.
###

You can enable separate annotations for different users, domains, and groups using Policies.

Advanced Mail Delivery Options

Click the **Advanced** button to reveal additional options for Advanced SMTP Settings, SMTP notifications, and the Received Header.



Advanced SMTP Settings

SMTP Pipelining: □ Disable

ESMTP: □ Disable

HELO required: ☑

Content rejected message: content rejected

Multiple recipient reject mode: All

Send EHLO: □ Enable

SMTP Notification (Advanced)

Select the type of notifications that are sent to the postmaster account.

☑ Resource

☑ Software

□ Bounce

□ Delay

□ Policy

□ Protocol

□ Double Bounce

Advanced SMTP Settings

You can configure these advanced SMTP settings:

SMTP Pipelining

Select the check box to disable SMTP Pipelining when delivering mail. Some mail servers may experience problems with SMTP command pipelining. You may have to disable this feature if required.

ESMTP

Select the check box to disable ESMTP (Extended SMTP) when delivering mail. Some mail servers may not support ESMTP. You may have to disable this option if experiencing problems.

> ***Warning*** *Disabling ESMTP disables TLS encryption on outgoing connections.*

HELO required

Enable this option to require clients to initiate their SMTP session with a standard HELO/EHLO sequence. It is recommended that you leave this feature enabled. It should only be disabled when experiencing problems with sending hosts that do not use a standard HELO message.

Content Reject Message

This is the text part of the SMTP 552 error message that is reported to clients when message content is rejected because the maximum message size has been exceeded.

Multiple Recipient Reject Mode

Indicates the reject handling of messages with multiple recipients. This option only applies to features with reject actions, for example, Malformed and Very Malformed Mail, Attachment Control, Content Scanning, Pattern Filters, OCF, Anti-Virus, and Intercept Anti-Spam features. This includes features defined in a policy.

- **All** – Reject the message if all recipients reject the message. If some but not all of the recipients reject the message, the message is discarded without notification to the sender for those recipients that rejected the message.
- **Any** – Reject the message if any recipient rejects the message.
- **Never** – The message is never rejected, regardless of any configured reject actions. For recipients that rejected the message, the message is discarded without notification to the sender.

Send EHLO

Always send EHLO when communicating with another server, even if their banner does not include ESMTP. Disable EHLO if you are experiencing communications problems with specific SMTP servers.

> ***Warning*** *Disabling EHLO disables TLS encryption on outgoing connections.*

SMTP Notification

Administrators can select the type of notifications that are sent to the postmaster account. Serious problems, for example, resource or software issues, are selected by default for notification.

Resource

Mail not delivered due to resource problems, for example, queue file write errors.

Software

Mail not delivered due to software problems.

Bounce

Send postmaster copies of undeliverable mail. If mail is undeliverable, a single bounce message is sent to the postmaster with a copy of the message that was not delivered. For privacy reasons, the postmaster copy is truncated after the original message headers. If a single bounce message is undeliverable, the postmaster receives a double bounce message with a copy of the entire single bounce message.

Delay

Inform the postmaster of delayed mail. In this case, the postmaster only receives message headers.

Policy

Inform the postmaster of client requests that are rejected because of policy restrictions.
The postmaster receives a transcript of the entire SMTP session.

Protocol

Inform the postmaster of protocol errors (client or server), or attempts by a client to execute unimplemented commands. The postmaster receives a transcript of the entire SMTP session.

Double Bounce

Send double bounced messages to the postmaster.

Received Header

The *Received Header* is the mail server information displayed in the Received: mail header of a message. You can modify the default WatchGuard XCS name to a generic identifier to prevent attackers from knowing the server details.

Mail Aliases

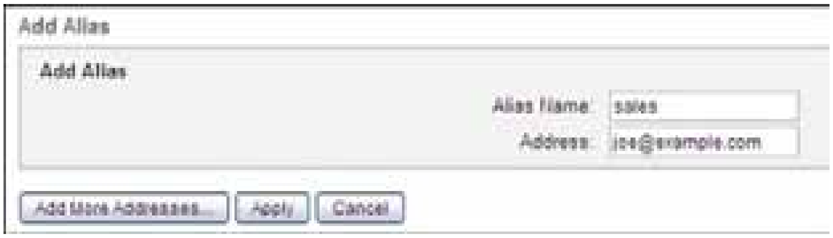
When mail is delivered locally, the delivery agent runs each local recipient name through the aliases database. If an alias exists, a new mail message is created for the named address or addresses. This mail message is returned to the delivery process to be mapped and routed. This process also occurs for local user accounts with a specified forwarder address. Local user accounts are treated as aliases in this case.

Local aliases are typically used to implement distribution lists, or to direct mail for standard aliases.

For example, the alias postmaster can resolve to the local mailboxes admin1@example.com, and admin2@example.com. For distribution lists, an alias called sales@example.com can be created that points to all members of the sales organization of a company.

To add a mail aliases:

1. Select **Configuration > Mail > Aliases**.
2. Click **Add Address**.



Alias Name: sales

Address: joe@example.com

3. In the **Alias Name** text box, enter a descriptive alias name.
4. In the **Address** text box, type the corresponding mail addresses for the alias.
5. Click **Add More Addresses** button to add multiple addresses for this alias.
6. Click **Apply**.

Upload Alias Lists

You can upload a list of aliases in a text file. The file must contain comma or tab separated entries.

Use this format:

```
[alias],[mail_address]
```

For example:

```
sales,fred@example.cominfo,mary@example.com
```

You must use a text editor to create the file alias.csv.

To update an alias file:

1. To download the alias list from the WatchGuard XCS, click **Download File**.
2. Open the file and update the alias list.
3. Click **Upload File** and upload the edited file to the WatchGuard XCS.

LDAP Aliases

Click **LDAP Aliases** to configure and search for aliases with LDAP. This allows you to search LDAP-enabled directories, for example, Active Directory, for mail aliases. See *LDAP Aliases* for more detailed information.

Mail Mappings

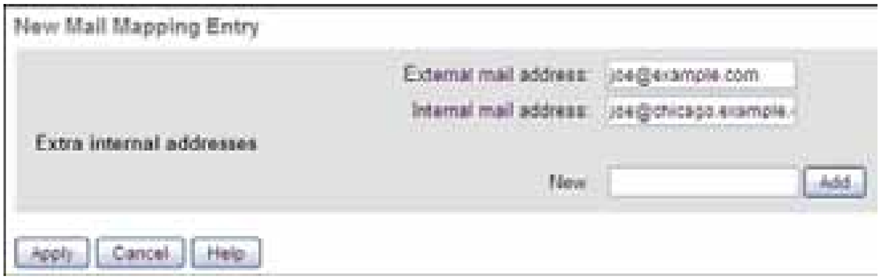
Mail Mappings map an external address to an internal address and vice versa. This is useful for hiding internal mail server addresses from external users. For mail originating externally, the mail mapping translates the address in the To: and CC: mail header field into a corresponding internal address that is delivered to a specific internal mailbox.

For example, you can redirect mail addressed to joe@example.com to the internal mail address joe@chicago.example.com. This delivers the message to the user’s preferred mailbox.

Mail originating internally has the address in the From:, Reply-To:, and Sender: header modified by a mail mapping to appear to come from the preferred external form of the mail address, joe@example.com.

To add a mail mapping:

1. Click **Configuration > Mail > Mapping**.
2. Click **Add**.



New Mail Mapping Entry

External mail address: joe@example.com

Internal mail address: joe@chicago.example.

Extra internal addresses

New:

3. In the **External mail address** text box, type the email address that you want to convert to the specified internal email address for incoming mail.
   The specified internal address is converted to this external address for outgoing mail.
4. In the **Internal mail address** text box, type the mapped address for the specified external address for incoming mail.
   The internal address is converted to the specified external address for outgoing mail.
5. In the New text box, type any additional internal mappings that are included in the outgoing mail conversion.

   Click **Add** for each entry.
6. Click **Apply**.

Upload Mapping Lists

You can upload a mappings list in a text file. The file must contain comma or tab separated entries.

Use this format:

```
[type ("sender" or "recipient")],[map_in],[map_out],[value ("on" or "off")]
```

For example:

```
sender,joe@chicago.example.com,joe@example.com,on
```

You must use a text editor to create the file mailmapping.csv.

To update a mapping file:

1. To download the mapping list from the WatchGuard XCS, click **Download File**.
2. Open the file and update the mapping list.
3. Click **Upload File** and upload the edited file to the WatchGuard XCS.

Mail Mapping as Access Control

You can block all incoming and outgoing mail messages that do not match a configured mail mapping. This feature makes sure that all incoming and outgoing mail matches a legitimate user as the destination or source of a message.

To configure access control:

1. Click **Preferences**.
2. Select the **Enable Mail Mapping Access Control** check box.
3. Click **Apply**.

Note these issues when you enable **Mail Mapping as Access Control**:

- Any users that send or receive mail require a mail mapping
- The mailer-daemon address bypasses the access control list and does not require a mapping
- The postmaster address bypasses the access control list and does not require a mapping
- These addresses must be added as mail mappings to make sure system-related messages can be sent out and received:
  - The admin user, for example, admin@example.com
  - Users configured to receive emailed reports
  - The user specified as the recipient in the Problem Reporting feature
- If you enable access control, all incoming and outgoing mail is blocked unless the user has a mapping listed in the mail mappings table.

Virtual Mappings

Virtual Mappings redirect mail addressed for one domain to a different domain. This process is performed without modifying the To: and From: headers in the mail, because virtual mappings modify the envelope-recipient address.

For example, you can accept mail for the domain @example.com and deliver it to @sales.example.com. This allows the system to distribute mail to multiple internal servers based on the Recipient: address of the incoming mail.

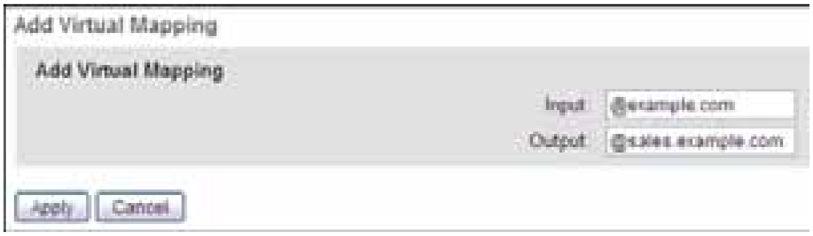
Virtual mappings are useful for acting as a wildcard mail mapping, for example, mail for example.com is sent to exchange.example.com. Virtual mappings are also useful for ISPs who need to accept mail for several domains, and situations where the envelope-recipient header must be rewritten for further delivery.

You should review the use of mail routes before you create virtual mappings because they are more appropriate for delivering mail to internal mail servers.

> **Note** *When you use Virtual Mappings, the Reject on Unknown Recipient and LDAP Recipient lookups are not performed for these mapped addresses. These email addresses are not rejected because the virtual mappings do not exist in an LDAP directory.*

To configure virtual mappings:

1. Select **Configuration > Mail > Virtual Mapping**.
2. Click **Add Virtual Mapping**.



Add Virtual Mapping

Add Virtual Mapping

Input: @example.com

Output: @sales.example.com

3. In the **Input** text box, type the domain or address to which incoming mail is directed.

   For example, `@example.com`.

4. In the **Output** text box, type the domain or address to which mail is redirected.

   For example, `@sales.example.com`

> ***Note*** *The domain that is virtually mapped or redirected must be defined in an "internal" DNS MX record to connect to this WatchGuard XCS.*

Upload Virtual Mapping Lists

You can upload a list of virtual mappings in a text file. The file must contain comma or tab separated entries.

Use this format:

```
[map_in],[map_out]
```

For example:

```
user@example.com,user
user@example.com,user@sales.example.com
@example.com,@sales.example.com
```

You must use a text editor to create the file virtmap.csv.

To update a mapping file:

1. To download the mapping list from the WatchGuard XCS, click **Download File**.
2. Open the file and update the mapping list.
3. Click **Upload File** and upload the edited file to the WatchGuard XCS.

LDAP Virtual Mappings

Click **LDAP Virtual Mappings** to configure and search for virtual mappings with LDAP. This allows you to search LDAP-enabled directories, for example, Active Directory, for virtual mappings.

See *LDAP Virtual Mappings* for more detailed information.

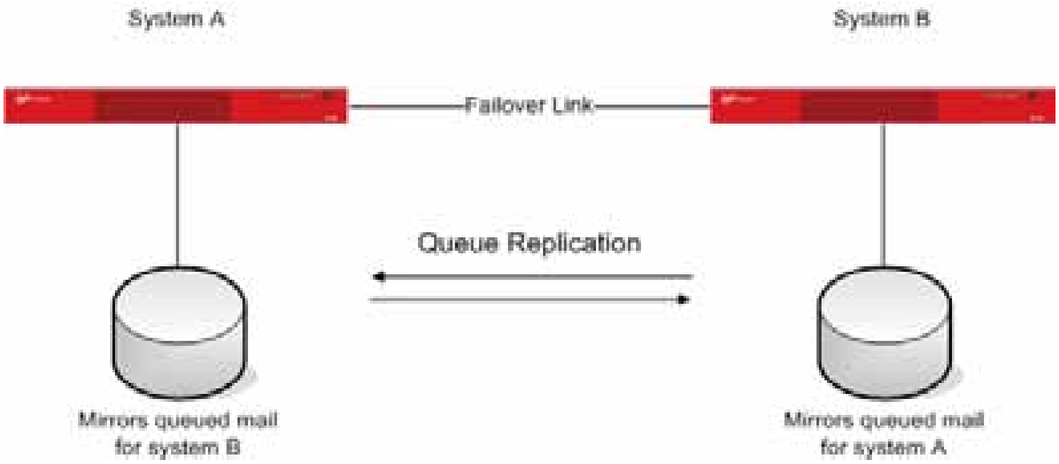
Queue Replication

The *Queue Replication* feature enables mail queue replication and failover between two WatchGuard XCS devices. In the event that the primary owner of a mail queue is unavailable, the mirror system can take ownership of the mirrored mail queue for delivery.

Queue replication actively copies any queued mail to the mirror system, ensuring that if one system should fail or be taken offline, the mirror system can take ownership of the queued mail and deliver it. If the source system successfully delivers the message, the copy of the message on the mirror server is automatically removed.

Without queue replication, a system with received and queued messages that have not been delivered can result in lost mail if that system suddenly fails. In large environments, this could translate into hundreds or thousands of messages.

In this diagram, *System A* and *System B* are configured to be mirrors of each other's mail queues.

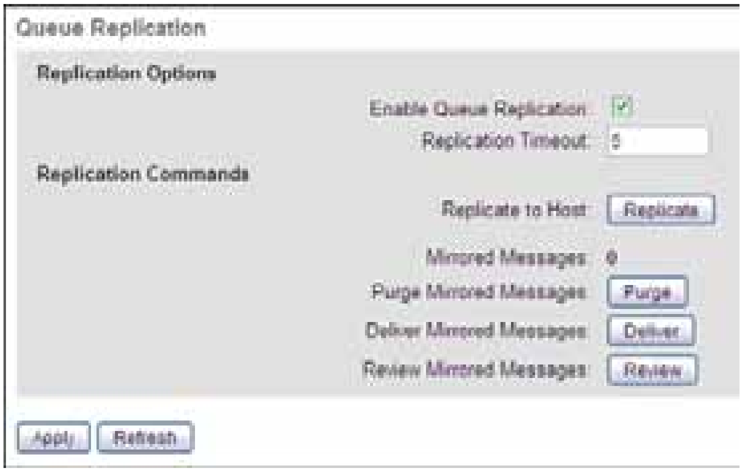

System A
System B
Failover Link
Queue Replication
Mirrors queued mail for system B
Mirrors queued mail for system A

When a message is received by *System A*, it is queued locally and a copy of the message is also immediately sent over the failover connection to the mirror queue on *System B*.

If *System A* fails, administrators can login to *System B* and take ownership of the queued mail to deliver it. Messages are exchanged between the systems to make sure that the mirrored mail queues are properly synchronized, which prevents duplicate messages from being delivered when a failed system comes back online.

To configure Queue Replication:

1. Select **Administration > Multi-System Management > Queue Replication**.



Queue Replication

Replication Options

Enable Queue Replication: ☑

Replication Timeout: 5

Replication Commands

Replicate to Host: Replicate

Mirrored Messages: 0

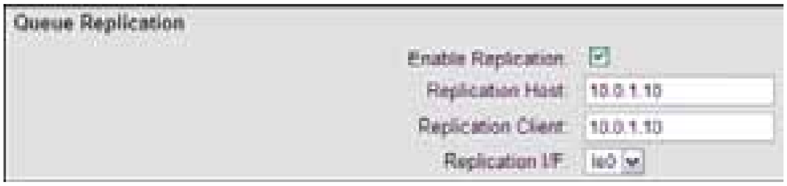
Purge Mirrored Messages: Purge

Deliver Mirrored Messages: Deliver

Review Mirrored Messages: Review

Apply Refresh

2. Select the **Enable Queue Replication** check box.
3. Click **Apply**.
4. Select **Configuration > Network > Interfaces**.
5. Go to the **Queue Replication** section.
   These options only appear in the Network settings page after you enable Queue Replication.



Queue Replication

Enable Replication ☑

Replication Host 10.0.1.10

Replication Client 10.0.1.10

Replication I/F le0

6. Select the **Enable Replication** check box.
7. In the **Replication Host** text box, type the IP address of the host that is backing up mail for this WatchGuard XCS.
   If you configure Queue Replication in a cluster, you can use the interface connected to the cluster network for replication. Specify the hostname of the host cluster system, for example, `SystemA`, in the address SystemA.example.com.
8. In the **Replication Client** text box, type the IP address of the client that is backing up its mail queue to this WatchGuard XCS.
   If you configure Queue Replication in a cluster, you can use the interface connected to the cluster network for replication. Specify the hostname of the host cluster system, for example, `SystemB`, in the address SystemB.example.com.
9. From the **Replication I/F** drop-down list, select the network interface to use for queue replication.

   This network interface must be connected to a secure network. We recommend that queue replication and clustering functions be run together on their own dedicated subnet.

10. Click **Apply**.

Import and Process Mirrored Messages

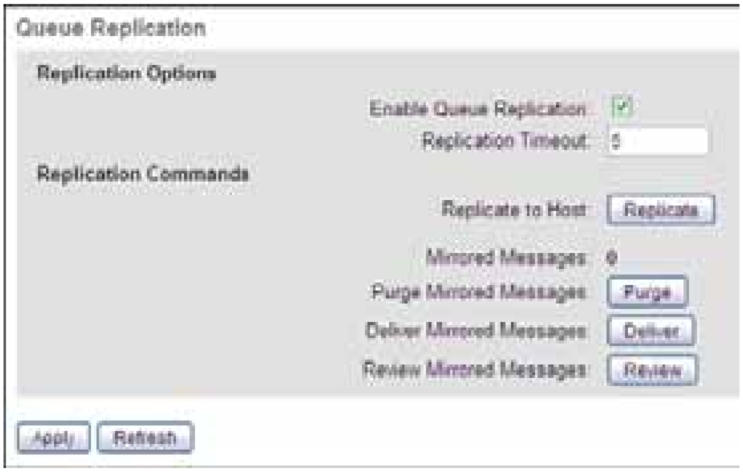
If you have two WatchGuard XCS devices that are mirroring each other's mail queues, and one of those devices fails, you must go to the mirror server and import the mirrored mail to make sure that it is processed and delivered.

To import the mirrored messages:

1. Make sure that the host system is unavailable.

   Before you import any mirrored mail, you must make sure that the host system is not processing mail. If you import and process the mirrored mail on the mirror system, this can result in duplicate messages if the host system starts to function again.

2. On the mirror device, select **Administration > Multi-System Management > Queue Replication**.
   The Queue Replication page appears.



Queue Replication

Replication Options

Enable Queue Replication: ☑

Replication Timeout: 5

Replication Commands

Mirrored Messages: 0

Replicate to Host: Replicate
Purge Mirrored Messages: Purge
Deliver Mirrored Messages: Deliver
Review Mirrored Messages: Review
Apply
Refresh

The **Mirrored Messages** value indicates the current amount of queued mail that is mirrored on this WatchGuard XCS.

3. Click the **Review Mirrored Messages** button to review any mail in the local queue that is mirrored from the source device.
4. To take ownership and process the mail that is mirrored for the source device, click **Deliver Mirrored Messages**.

> ***Warning*** *Do not click the **Deliver Mirrored Messages** button unless you are certain that the source system is unable to deliver mail.*

You can also perform these functions from the Queue Replication page:

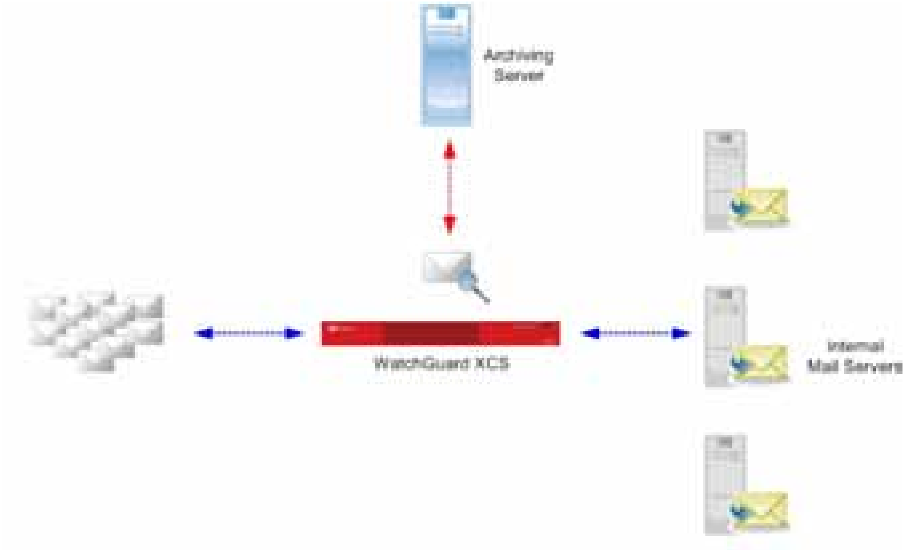
- In the **Replication Timeout** text box, type the time interval, in seconds, to contact the host system before timing out. The default is 5 seconds.
- Click **Replicate to Host** to replicate the queue to the mirror host system immediately. The mail queues are automatically updated when a message is first received, and the queues are also synchronized at regular intervals.
- Click the **Purge Mirrored Messages** button to delete any mail messages in the local mirror queue. These are the files that are mirrored for another host device.

Message Archiving

Archiving support allows organizations to define additional mail handling controls for inbound and outbound mail. These features are especially important for organizations that must archive certain types of mail for regulatory compliance or other corporate security policies.

Mail is categorized and selectively archived for different levels of importance. By providing the ability to classify and archive messages at different levels, mail of high importance or compliance classification can be archived, while you can configure different actions for mail of lower importance. These features also prevent the waste of unnecessary resources by ignoring spam messages and other types of unwanted mail when archiving messages.

The WatchGuard XCS integrates with third-party archiving servers to archive email messages with pattern filters that classify messages and route them to the appropriate archiving server or an archive email address, while still delivering the email to the original recipients. Mail headers added to an archived message by the WatchGuard XCS allow you to customize archiving services for efficient retrieval of archived messages.



You can use archiving with Pattern Filters, the Objectionable Content Filter, and Content Scanning. When the WatchGuard XCS receives a message, these features search for text within a message and its attachments. When this text is found, an action is performed to classify the message for archiving into one of three categories: **Archive High**, **Archive Medium**, and **Archive Low**.

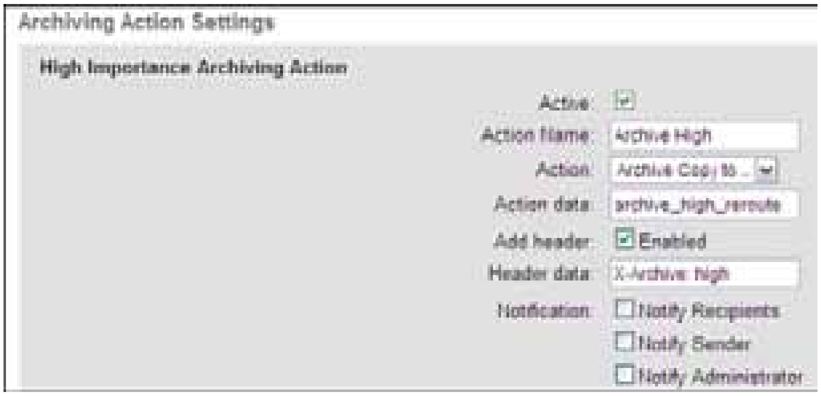
The WatchGuard XCS then applies the archiving action for each category. For example, messages categorized as **Archive High** can have an action of **Archive copy to**, with the action data identifying the archiving email address or the mail route to which to archive mail to.

Configure Message Archiving

To configure Message Archiving:

1. Select **Configuration > Mail > Archiving**.

   Configuration fields for three classifications of archiving appear for **High**, **Medium**, and **Low Importance** archiving actions.



Archiving Action Settings

High Importance Archiving Action

Active: ☑

Action Name: Archive High

Action: Archive Copy to ...

Action data: archive_high_reroute

Add header: ☑ Enabled

Header data: X-Archive: high

Notification: □ Notify Recipients

□ Notify Sender

□ Notify Administrator

2. Select the **Active** check box.
3. In the **Action Name** text box, type a name to display as the archiving action for the Pattern Filter, Objectionable Content, and Content Scanning features.
4. From the **Action** drop-down list, select **Archive copy to** to send the message to an archive server.
5. In the **Action Data** text box, type an email address or the name of the mail route for the destination archiving server.

   If you enter an email address, this is a mailbox that contains all archived messages. Your archiving server can pull its data for the archived messages from this mailbox.

   To use a mail route to route mail to the archiving server, set the **Action Data** to **archive_high_reroute**, **archive_medium_reroute**, or **archive_low_reroute** as required.

   You must create a corresponding mail route on the **Configuration > Mail > Routing** page. Mail routes are not required if you archive to an email address.

6. To add an archive header to the message when it is sent to the destination archive server, select the **Add header Enabled** check box.

   This allows the archiving server to store that message according to its classification in the header and allow for more efficient retrieval of the message.

7. In the **Header data** text box, enter the header that is added to the message header.

   For example, `X-Archive: high`

8. To send a notification to when a message is archived, select **Notify Recipients**, **Notify Sender**, or **Notify Administrator**.
9. Click **Apply**.

Define Mail Routes for Archiving

When you use the mail routing method for archiving messages, you must define mail routes to the archiving server to make sure that the WatchGuard XCS knows where to send messages for the appropriate message archiving classification.

For each archiving classification, a corresponding mail route must created:

For archive_high_reroute, use: `.archive_high_reroute`

For archive_medium_reroute, use: `.archive_medium_reroute`

For archive_low_reroute, use: `.archive_low_reroute`

To set up mail routes for archiving:

1. Select **Configuration > Mail > Routing**.
2. Type the domain, for example,`.archive_high_reroute`, and type the destination address of the archiving server.
3. Click **Add**.

> ***Note*** *Mail routes are not required when you archive to an email address.*

Configure Content Control Filters for Archiving

To classify messages for archiving, you must configure the content control features, for example, Pattern Filters, Objectionable Content filtering, and Content Scanning, to search for text in a message or its attachment. The corresponding action is the archive classification, for example, “Archive High”.

Configuring Pattern Filters for archiving

1. Select **Security > Content Control > Pattern Filters**.
2. Click **Add**.
3. Create a pattern filter for the required specific text.

   For example, search for an inbound message subject that starts with the word “Compliance”.
4. Set the **Action** to the appropriate archive action, for example, **Archive High**.
5. Click **Apply**.

Configuring OCF for Archiving

The Objectionable Content Filter can be used to classify and archive messages. You can create custom dictionaries for content specific to your organization. When the OCF feature finds a word from these dictionaries, an archive action is applied.

1. Select **Security > Content Control > Objectionable Content**.
2. Enable the OCF feature.
3. Select your customized dictionary file, for example, “Archive”.
4. Set the **Action** to the appropriate archive action for this dictionary file, for example, **Archive Low**.
5. Click **Apply**.

Configure Policies for Archiving

You can use policies to customize archive actions for different domains or groups of users. When you create a policy, the Content Scanning feature provides actions for archiving when specific text is found in an attachment. The Content Scanning feature requires a dictionary file to match against the attachment content, and a corresponding archiving action to perform.

1. To configure a policy definition:
2. Enable Content Scanning globally from **Security > Content Control > Content Scanning**.
3. Select **Security > Policies**.
4. Select the **Content Control** tab.

5. In the **Content Scanning** section for inbound messages, select the **Compliance Dictionary** to use for matching text, for example, “Archive”.
6. Set the **Action** to the appropriate archive action for this dictionary file, for example, **Archive Medium**.

Customize Archive Headers with Policies

For each policy definition, you can customize the **Archive Header** for each archiving classification.
This is configured in the **Email** policy tab.

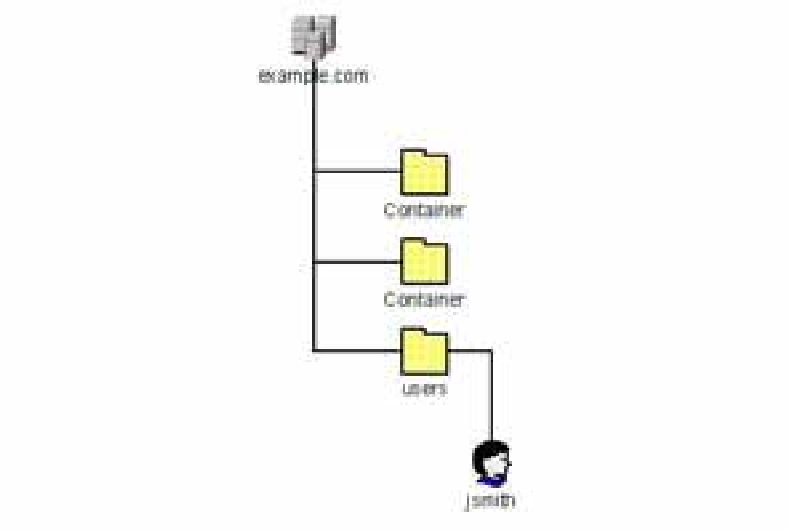
7 LDAP and Directory Services

LDAP Overview

The WatchGuard XCS utilizes *LDAP (Lightweight Directory Access Protocol)* services for accessing directories for user and group information. LDAP is used for mail routing, group and user lookups for policies, user lookups for mail delivery, alias and virtual mappings, and remote authentication. LDAP is designed to provide a standard for efficient access to directory services using simple data queries. Most major directory services, for example, Active Directory, support LDAP but each differs in their interpretation and naming convention syntax. Other types of supported LDAP services include OpenLDAP and iPlanet.

Naming Conventions

The method for which data is arranged in the directory service hierarchy is a unique *Distinguished Name*. This diagram is an example of a Distinguished Name in Active Directory:



```
cn=jsmith,dc=example,dc=com
```

In this example, “cn” represents the Common Name, and “dc” is the Domain Component. The user jsmith is in the users container. The domain component is analogous to the FQDN domain name, in this example, example.com.

> **Note** *For all LDAP Directory features, you must make sure you enter values specific to your LDAP environment and schema.*

Common names are not always unique. Another way to reference user objects is by their login name that is a unique identifier within an organization. Another DN for John Smith is:

```
UID=jsmith,CN=Canada,DC=example,DC=com
```

This second DN is different from the first example, but points to the same user object, and uses a different RDN name to identify the local entry. The root of the directory is called the base DN. The base DN is typically set to closely match the DNS name for the server. The base DN uses the Domain Components (dc) attribute to distinguish its DNS zones. The administrator may want to make the directory structure different than the DNS structure to have more flexibility in its design. Similar to DNS, the TLD is one zone with the registered name of the domain is another zone.

```
DNS name: example.com
Base DN: dc=example, dc=com
```

The objectClass attribute defines the entry rules. The objectClass attribute is mandatory for all entries in the directory. It describes the content of the entry by specifying which other attributes are mandatory, and which are optional. An entry is assigned multiple objectClass attribute pairs. The schema of the directory determines which objectClasses are available. Some examples of common objectClasses are:

objectClass group

objectClass computer

objectClass user

objectClass container

LDAP Schema

The directory schema defines the rules the directory can use when to save and store the data. The schema governs what types of objects are populated, which attributes are allowed, the structure of those attributes, and what the valid compare operators are. “Greater than”, “less than”, and “equal to” are common compare operators. The minimum set of schema objects required by LDAP allows us to browse the directory structure. A directory schema can be extended beyond its default design to conform to the data requirements of an organization. Most directories have a single schema that is shared throughout the entire directory. Others directories can have different schemas for different sections of the directory.

LDAP Components

LDAP is a term commonly used in the technology field to describe a group of functions. There are several different components that encompass LDAP technology.

Clients

The LDAP client used to query a directory can be a stand-alone piece of software, or can it can be integrated into other applications. When integrated, LDAP works seamlessly, and its functions are unknown to the user or administrator. LDAP is used by large organizations because of its flexibility between the client and the server, and its ease of client integration with existing software. Because the naming conventions are the same for directory servers, LDAP clients can support many different LDAP implementations from different vendors.

Protocol

LDAP uses TCP/IP for its interface to the network and its hosts. For LDAP to communicate with a directory server, it must establish a TCP session. The LDAP protocol encodes the attribute value data that passes between the server and client. Any LDAP client can speak to any LDAP enabled server because of the standard application programming interface (API). The LDAP protocol also supports the use of Unicode UTF-8 to support non-English languages.

Operations

LDAP has very few operations available to lower the complexity of the protocol for the client programs. These are categories of the operations and their functions:

Category	LDAP Operations
Client Session	Bind, unbind, abandon
Query and Retrieval	Search and compare
Modification	Add, modify, modifyRDN, delete
Extended	Extended

Client Session Operations

Session operations control access to the directory server using the bind, unbind, and abandon operations. When a client binds to the directory server, its identity can be used to decide the level of permissions the client has when accessing the objects. The bind operation is similar to a login. Any other operation you use to interact with the server requires a successful bind to the directory. To perform this operation requires a user name and password, or you can use an anonymous bind.

> **Note** *For most LDAP servers, binding anonymously to the server does not allow you access to all the information you would be able to obtain if you had used an actual login and password.*

The unbind operation closes the LDAP session to the server, and the abandon operation allows the client to cancel an outstanding operation request.

Query Operations

The query operations are used the when applications are integrating with a directory server. These operations search and retrieve the information from the directory server. The "search" operation is most frequently used because you typically do not know the location of the information you want to obtain. Through the use of string parameters, an LDAP client can perform sophisticated queries to search for data within the directory. The "compare" operation can take a value and verify it against a directory object or attribute. The LDAP client sends the values of the attribute pair, and the server responds with a "success" if it matches, or a failure if it does not match.

You can use filter operations in LDAP queries to help narrow down or widen the scope of the search. You can use these boolean operators when you perform a query:

LDAP Filter Character	Boolean Operator
&	AND
|	OR
!	NOT

These operators precede the filter they modify. A normal search string to find all user objects is:

```
(objectCategory=person)
```

A search string to find a specific user object is:

```
(&(objectCategory=person)(name=John Smith))
```

A search string to return all user objects except for those in the admin group "admins" is:

```
(objectCategory=person)(!(&(objectCategory=person)(memberOf=admins)))
```

Modification Operations

Modification operations allow changes to be made to the data within the directory. Operations, for example, "add", "modify", and "delete", are standard and self-explanatory. The modifyRDN operation allows the client to change the name of an entry and to move the entry to a different container. Depending on the access permissions (determined when binding to the directory), some modifications are not allowed. For example, a read-only branch of the directory does not allow any of the modification operations to be processed.

Extended Operations

Extended operations are unique for each directory server and client. They are used as a placeholder for custom protocol expansions but still defines the syntax to be used.

Security

The LDAP protocol supports the use of SSL (Secure Sockets Layer) for its data encryption privacy. Encrypting the session between the client and the directory server makes sure that computers sniffing the traffic in the network cannot read any of the data within the session. Authentication is handled by the client bind operation. After a successful bind to the directory server, the authorization dictates which objects are available to the user. This can also include an anonymous user situation where no bind operation was performed before a query.

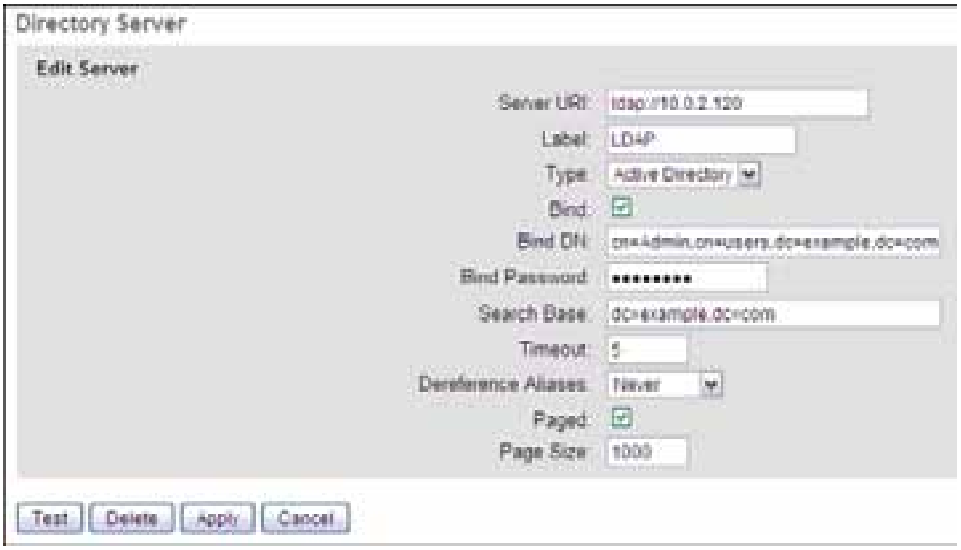
Directory Servers

The WatchGuard XCS uses the directory servers you specify for all LDAP functions. This includes user and group membership confirmation, authentication, and mail routing.

To configure Directory Servers:

1. Select **Configuration > LDAP > Directory Servers**.
   The Directory Server page appears.
2. To configure a new directory server, click **Add**.

   To modify an existing server, click **Edit**.



Server URI:	ldap://10.0.2.120
Label:	LDAP
Type:	Active Directory
Bind:	☑
Bind DN:	cn=Admin,cn=users,dc=example,dc=com
Bind Password:	●●●●●●●●●
Search Base:	dc=example,dc=com
Timeout:	5
Dereference Aliases:	Never
Paged:	☑
Page Size:	1000

3. In the **Server URI** text box, type the URI (Uniform Resource Identifier) address for the server. For example, `ldap://10.0.2.120`.

   If you use SSL with the LDAP server directory, type `ldaps` instead of `ldap`.

   To query an Active Directory global catalog, add the port number 3268 to the server URI. For example, `ldap://10.0.2.120:3268`.
4. In the **Label** text box, type a name or alias for the LDAP server.
5. From the **Type** drop-down list, select the type of LDAP server you specified.

   If you use an OpenLDAP or iPlanet server, select **Others**.

6. Select the **Bind** check box.
7. In the **Bind DN** text box, type the DN (Distinguished Name) for your directory server.

   For example, for Active Directory, type: `cn=Administrator,cn=users,dc=example,dc=com`

   Older Windows login names, for example, `DOMAIN/Administrator`, are also supported. Make sure that you select a bind DN specific to your environment.

   In Active Directory, if you use an account other than Administrator to bind to the LDAP server, the name must be specified as the full name, not the account name. For example, use “John Smith” instead of “jsmith”.

8. In the **Bind Password** text box, type the password to use for the LDAP server.
9. In the **Search Base** text box, type the default search base for account lookups.
   For example, `dc=example,dc=com`.
10. In the **Timeout** text box, type the maximum amount of time, in seconds, to wait for the search to complete.
    You can set the timeout value to between 1 and 100 seconds.
11. From the **Dereference Aliases** drop-down list, select the method to use for to dereference aliases in a directory search:

    - **Never** – Aliases are never dereferenced.
    - **Searching** – Aliases are dereferenced in subordinates of the base object, but not when the base object of the search is found.
    - **Finding** – Aliases are only dereferenced when the base object of the search is found.
    - **Always** – Aliases are dereferenced when the base object of the search is searched for and found.

12. To enable paging support for an Active Directory server, select the **Paged** check box.

    When a query is sent to an LDAP server, the amount of information returned could contain thousands of entries and sub-entries. Paging enables the information from the LDAP server to be retrieved in more manageable sections to control the rate of data return.

13. In the **Page Size** text box, type the maximum number of entries to be returned in a query to the Active Directory server. The default setting is 1000.

    If you do not type a new setting, the default value of 1000 is used. The setting you select must match the size configured in the LDAP query policy for the Active Directory server.

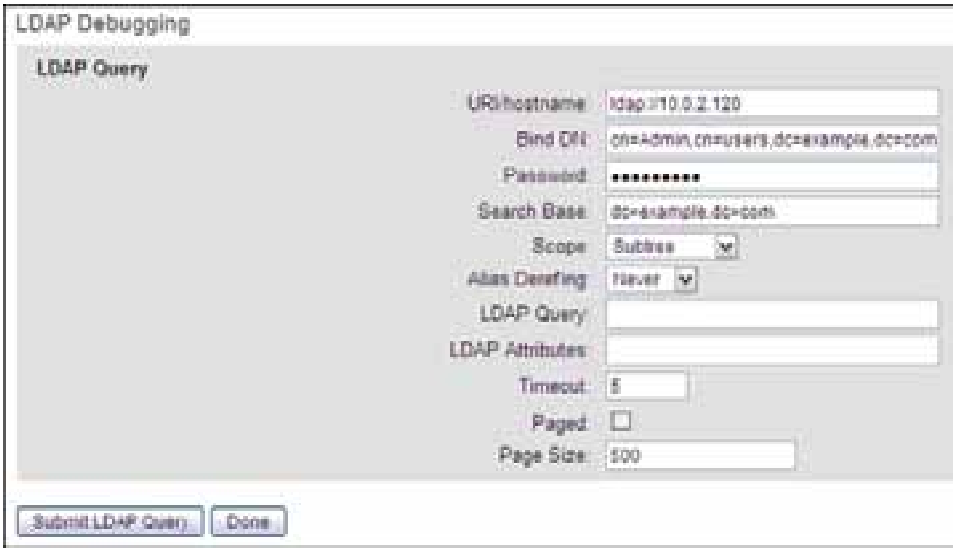
14. Click **Test**.
    A test query is sent to the LDAP server to test your LDAP settings.
15. Click **Apply**.

> ***Note*** *If you delete an LDAP server, this removes all additional configuration items based on that server, for example, Directory Users, Groups, and Aliases.*

Test LDAP Servers

To test your LDAP server configuration:

1. Select **Configuration > LDAP > Directory Servers**.
   The Directory Server page appears.
2. Click **Test**.
   The LDAP Debugging page appears.



URI/hostname: ldap://10.0.2.120

Bind DN: cn=Admin,cn=users,dc=example,dc=com

Password: ••••••••••

Search Base: dc=example,dc=com

Scope: Subtree

Alias Derefing: Never

LDAP Query:

LDAP Attributes:

Timeout: 5

Paged: □

Page Size: 500

3. Click **Submit LDAP Query**.

   If the remote server does not respond, this error message appears:

   ```
   ldap_bind: Can't contact LDAP server (81)
   ```

   If the user you used to bind to the LDAP tree does not have enough permissions, this message appears:

   ```
   ldap_bind: Invalid credentials (49)

   additional info: 80090308: LdapErr: DSID-0C09030B, comment: 
   AcceptSecurityContext error, data 525, v893
   ```

   This is typically caused by a wrong user name or password.

   If the search base you specify does not exist, this message appears:

   ```
   # extended LDIF

   #

   # LDAPv3

   # base  with scope sub

   # filter: (objectClass=*)

   # requesting: ALL

   #


   # search result

   search: 2

   result: 32 No such object

   matchedDN: DC=example,DC=com

   text: 0000208D: NameErr: DSID-031001BD, problem 2001

   (NO_OBJECT), data 0, best match of:

           'DC=example,DC=com'
   ```

```
# numResponses: 1
```

Search the LDAP Tree

You can choose a specific type of object to find in the LDAP query field. For example, if you want to search for users, use the filter: `(ObjectCategory=person)`. This displays all users within the specified search base.
If you specify a search filter in the LDAP Query field, this displays every single record with all the attributes associated with the selected search filter.

To narrow the search results, you can specify LDAP attributes to format the display so that only certain attributes are displayed for each returned object. In addition, there is an attribute called ObjectClass and the value is also equal to “user” in each user object, but `(ObjectClass=user)` returns a computer object as well.

To search for all user objects (this includes group information) with the email domain example.com, and display the mail attribute of each object in the result, use this query:

```
(mail=*example.com)
```

The results of the query are similar to this message:

```
# extended LDIF


# LDAPv3
# base  with scope sub
# filter: (mail=*@example.com)
# requesting: mail
#


# techsupport, users, example.com
dn: CN=techsupport,OU=users,DC=example,DC=com
mail: techsupport@example.com


# sales, users, example.com
dn: CN=sales,OU=users,DC=example,DC=com
mail: sales@example.com


# Joe TS. Smith, users, example.com
dn: CN=Joe TS. Smith,OU=users,DC=example,DC=com
mail: jsmith@example.com


# Ken R. Simon, users, example.com
dn: CN=Ken R. Simon,OU=users,DC=example,DC=com
mail: ksimon@example.com
```

```
# Andrew Y. Roberts, users, example.com
dn: CN=Andrew Y. Roberts,OU=users,DC=example,DC=com
mail: aroberts@example.com

# Kathy J. Norman, users, example.com
dn: CN=Kathy J. Norman,OU=users,DC=example,DC=com
mail: knorman@example.com

# search result
search: 2
result: 0 Success

# numResponses: 7
# numEntries: 6
```

If you want to search for users only, use this LDAP Query:
`(&(ObjectCategory=user)(mail=*example.com))`

If you want to display the login name for each object returned, use `sAMAccountName` as the LDAP attribute instead of `mail`.

The results of the query are similar to this message:

```
# techsupport, users, example.com
dn: CN=techsupport,OU=users,DC=example,DC=com
sAMAccountName: techsupport
```

Directory Users

Use the *Directory Users* feature to import user account and group membership data from LDAP-based directory servers. This information is used by the Intercept Anti-Spam *Reject on Unknown Recipient* feature to provide LDAP lookups for valid email addresses and to import group membership information for policies.

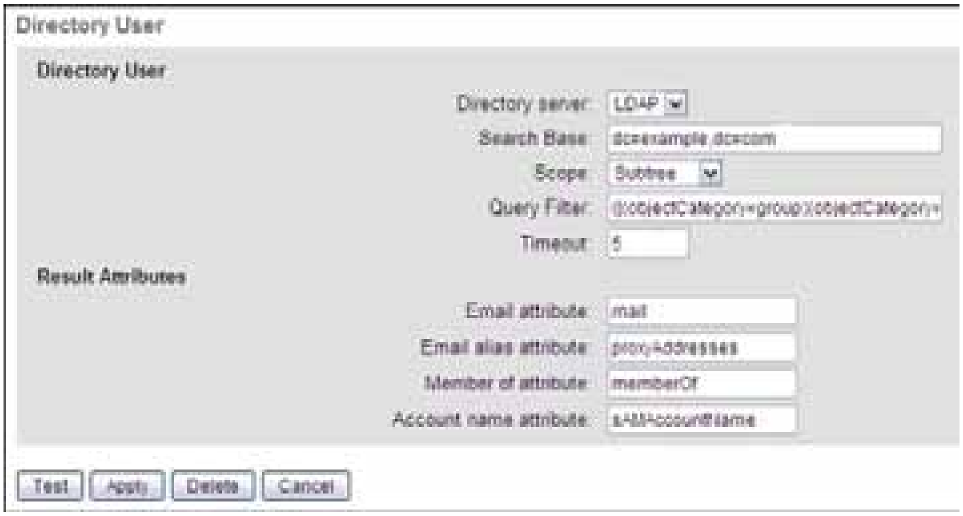
> ***Note*** *Only groups that the imported users belong to are imported. Group Policy must be enabled before you import users and groups if you use the information for Group policies.*

You can create local mirror accounts to allow directory-based users to view and manage quarantined mail for the Spam Quarantine feature.

To configure Directory Users:

1. Select **Configuration > LDAP > Directory Users**.
   The Directory User page appears.

2. Click **Add**.



Directory User

Directory User

Directory server: LDAP

Search Base: dc=example,dc=com

Scope: Subtree

Query Filter: (|(objectCategory=group)(objectCategory=

Timeout: 5

Result Attributes

Email attribute: mail

Email alias attribute: proxyAddresses

Member of attribute: memberOf

Account name attribute: sAMAccountName

3. From the **Directory Server** drop-down list, select a server to perform the search.
4. In the **Search Base** text box, type a **Search Base** string with information specific to your LDAP hierarchy.

   For example: `cn=users,dc=example,dc=com`.

5. From the **Scope** drop-down list, select the scope of the search.

   - **Base** – Searches the base object only.
   - **One Level** – Searches objects beneath the base object, but excludes the base object.
   - **Subtree** – Searches the entire subtree of which the base distinguished name is the topmost object, and includes the base object.

6. In the **Query Filter** text box, type a filter to return the user account information.

   For example, for Active Directory, type:
   `(|(|(objectCategory=group)(objectCategory=person))(objectCategory=publicFolder))`

   This query filter includes mail-enabled Exchange public folders to prevent them from being rejected if *Reject on Unknown Recipient* is enabled.

   For iPlanet and OpenLDAP, type:`(objectClass=person)`

7. In the **Timeout** text box, type the maximum interval, in seconds, to wait for the search to complete.
   You can enter values from 1 to 100 seconds.
8. In the **Email attribute** text box, type the attribute that identifies the user’s email address.

   For Active Directory, iPlanet, and OpenLDAP, type: `mail`.

9. In the **Email alias attribute** text box, type the attribute that identifies the user’s alternate email addresses.

   For Active Directory, type: `proxyAddresses`.

   For iPlanet, type: `Email`.

   For OpenLDAP, leave this field blank.

10. In the **Member Of** text box, type the attribute that identifies the groups that the user belongs to for group policy resolution.

    For Active Directory, type: `memberOf`.

    For iPlanet, type: `Member`.

    For OpenLDAP, leave this field blank.

11. In the **Account Name Attribute** text box, type the attribute that identifies a user's account name for login.

    For Active Directory, type: `sAMAccountName`.

    For iPlanet, type: `uid`.

    For OpenLDAP, type: `cn`.

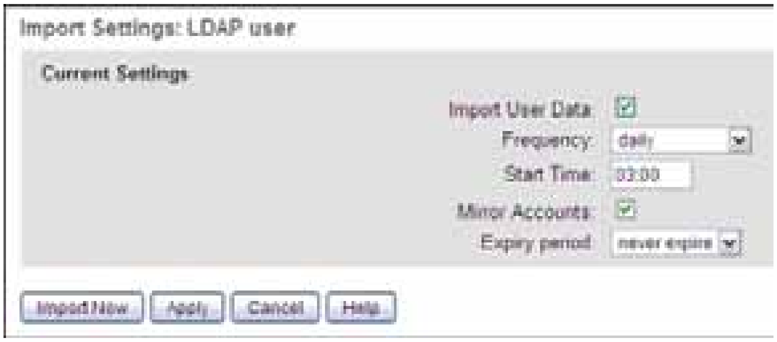
12. Click the **Test** button to test your LDAP settings.
13. Click **Apply**.

Import Settings

You can automatically import LDAP user data on a scheduled basis to stay synchronized with the LDAP directory.

To import LDAP users and groups:

1. Select **Configuration > LDAP > Directory Users**.
   The Import Settings: LDAP User page appears.
2. Click **Import Settings**.



Import Settings: LDAP user

Current Settings

Import User Data: ☑
Frequency: daily
Start Time: 03:00
Mirror Accounts: ☑
Expiry period: never expire

3. To enable automatic import of LDAP user data, select the **Import User Data** check box.

   Automatic import makes sure that your imported LDAP data remains current with the information on the LDAP directory server.

4. In the **Frequency** drop-down list, select the frequency of LDAP imports.

   - **Hourly**
   - **Every 3 Hours**
   - **Daily**
   - **Weekly**
   - **Monthly**

5. In the **Start Time** text box, type the start time for the import in the format hh:mm.

For example, to schedule an import at midnight, type: `00:00`.

6. Click **Apply**.
7. Click **Import Now** to immediately begin the import of users.

   To view the progress of LDAP imports, select **Activity > Logs > System**.

Mirror LDAP Accounts

To provide local account access, you can mirror existing LDAP accounts, which creates a local account on the WatchGuard XCS for each imported user.

This allows directory-based users to view and manage quarantined messages for the Spam Quarantine and the Trusted/Blocked Senders List features.

> ***Note*** *You cannot use mirror accounts as local mail accounts.*

To configure mirror users:

1. Select the **Mirror accounts** check box.
2. From the **Expiry period** drop-down list, select an expiration period for mirrored accounts.

   If the user no longer exists in the LDAP directory for the specified period of time, the local mirrored account is deleted. This option only applies to a mirrored account, not accounts used for the *Reject on Unknown Recipients* feature.
3. Click **Apply**.
4. Click **Import Now** to immediately begin the import of users and create mirrored accounts.

   To view the progress of LDAP imports, select **Activity > Logs > System**.

   To view mirrored accounts, select **Administration > Accounts > Mirrored Accounts**.

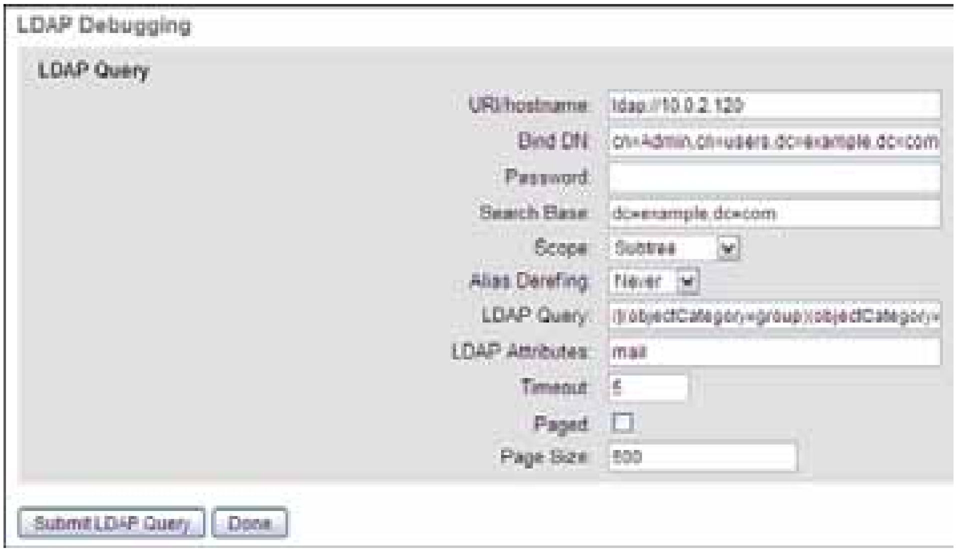
Test Directory Users

There are four main attributes specific to Active Directory that the WatchGuard XCS uses for mail processing:

- mail
- proxyAddresses
- memberOf
- sAMAccountName

To make sure that the information imported is properly accepted by the WatchGuard XCS, test the LDAP query and attributes before you import LDAP users.

1. Select **Configuration > LDAP > Directory Users**.
   The Directory User page appears.
2. Click **Test**.
   The LDAP Debugging page appears.



LDAP Debugging

LDAP Query

URI/hostname: ldap://10.0.2.120

Bind DN: cn=Admin,cn=users,dc=example,dc=com

Password:

Search Base: dc=example,dc=com

Scope: Subtree

Alias Derefing: Never

LDAP Query: (|(objectCategory=group)(objectCategory=

LDAP Attributes: mail

Timeout: 5

Paged: □

Page Size: 500

3. Test the *mail* attribute with this query:
   - For **LDAP Query**, use the default value: `(|(objectCategory=group)(objectCategory=person))`.
   - For the **LDAP attributes** text box, use the `mail` attribute.
4. Click **Submit LDAP Query**.

The results display the requested attribute (mail). The WatchGuard XCS uses this as the account name to create mirrored accounts. There is only one email address returned for each user even though a user can have multiple messages in an Active Directory/Exchange environment.

To view or modify the primary user in Active Directory:

1. Open **Active Directory Users and Computers**.
2. Double click on the user.
3. Click the **Email Addresses** tab.
   The Primary account is the one highlighted with type SMTP.
4. To change the Primary email account, select the address you want to make primary and click **Set As Primary**.
5. Test the **proxyAddresses** attribute with this query:
   - For **LDAP Query**, type: `(|(objectCategory=group)(objectCategory=person))`
   - For the **LDAP attributes** field, type: `proxyAddresses`
6. Click **Submit LDAP Query**.

The SMTP item in uppercase letters is the primary address (the same as the **mail** attribute).

The **proxyAddresses** attribute is used to implement the *Reject on Unknown Recipients* feature.
The WatchGuard XCS uses this attribute for the mail attributes and to process any additional email addresses (this includes aliases) associated with the users and groups.

Test the **memberOf** attribute with this query:

1. For **LDAP Query**, type:`(|(objectCategory=group)(objectCategory=person))`
2. For the **LDAP attributes** text box, type: `memberOf`

3. Click **Submit LDAP Query**.

The **sAMAccountName** attribute is used as the login name by the WatchGuard XCS when it authenticates with the Active Directory server. This attribute is not necessarily equivalent to the email name. To locate the **sAMAccountName** attribute in Active Directory:

1. Go to user properties in **Active Directory Users and Computers**.
2. Click the **Account** tab.
3. The **sAMAccountName** corresponds to the **User Login Name**.

LDAP Aliases

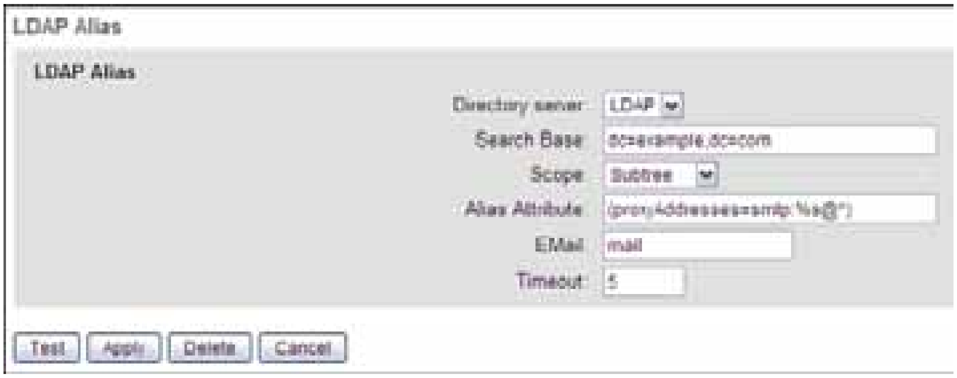
Use *LDAP Aliases* to search LDAP-enabled directories for user mail aliases. If an alias exists, a new mail message is created for the named address or addresses. This mail message is returned to the delivery process and mapped, routed, and processed.

> **Note** *LDAP Aliases have only been tested with Active Directory, and the examples shown are for Active Directory LDAP implementations. In most cases, Active Directory already performs its own internal alias translations and configuring LDAP Aliases is not required.*

See *Mail Aliases* for more detailed information on Mail Aliases.

To configure LDAP Aliases:

1. Select **Configuration > LDAP > Aliases**.
   The LDAP Alias page appears.
2. Click **Add**.



LDAP Alias

LDAP Alias

Directory server: LDAP
Search Base: dc=example,dc=com
Scope: Subtree
Alias Attribute: (proxyAddresses=smtp:%s@*)
EMail: mail
Timeout: 5

3. From the **Directory Server** drop-down list, select a server to perform the search.
4. In the **Search Base** text box, type a **Search Base** string with information specific to your LDAP hierarchy.

   For example: `cn=users,dc=example,dc=com`.

5. From the **Scope** drop-down list, select the scope of the search.

   - **Base** – Searches the base object only.
   - **One Level** – Searches objects beneath the base object, but excludes the base object.
   - **Subtree** – Searches the entire subtree of which the base distinguished name is the topmost object, and includes the base object.

5. In the **Alias Attribute** text box, type the attribute that defines the alias mail addresses for a user.

   For example, for Active Directory, type: `(proxyAddresses=smtp:%s@*)`
6. In the **Email** attribute text box, type the attribute that returns the user's email address.
7. For example, for Active Directory, type: `mail`
8. In the **Timeout** text box, type the maximum interval, in seconds, to wait for the search to complete.
   You can enter values from 1 to 100 seconds.
9. Click the **Test** button to perform a test of the LDAP Aliases configuration.
10. Click **Apply**.

LDAP Web Users

The *LDAP Web Users* feature allows LDAP-authenticated clients to utilize the system's Web Proxy feature. These clients must use a login and password to authenticate to an LDAP server before they can use the Web Proxy. LDAP Authentication allows the WatchGuard XCS to authenticate the user directly to an LDAP directory server without the need to create a local account.

When a user successfully authenticates with the LDAP server, the information is saved in an LDAP authentication cache on the system for 300 seconds. Any subsequent LDAP requests go to the cache instead of the LDAP server. This enables a faster response and prevents the LDAP server from being overloaded with authentication requests. After 300 seconds, the Web Proxy authenticates directly to the LDAP server again and caches the results if the authentication is successful.

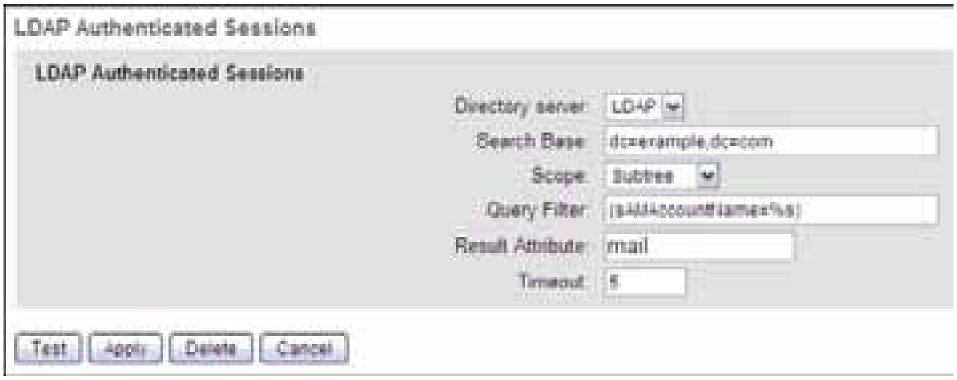
To configure LDAP authentication for web users:

1. Select **Configuration > LDAP > Web Users**.
   The LDAP Authenticated Sessions page appears.
2. Select a method, and then click **Add** to add an entry.
   You can only use one method, Bind or Query Direct, for all defined LDAP servers. You cannot use both at the same time.

> ***Note*** *The Bind method only works with Active Directory and iPlanet implementations. The Query Direct method only works with OpenLDAP.*

- **Bind** – The Bind method uses the User ID and password to authenticate on a successful bind. The Query Filter must specify the User ID with a %s variable. For example, for Active Directory, use `(sAMAccountName=%s)` for the Query Filter. Use `mail` for the Result Attribute. For iPlanet, use `uid=%s` for the Query Filter, and `mail` for the Result Attribute.
- **Query Directly** – The Query Direct method queries the LDAP server directly to authenticate a user ID and password. The Query Filter must specify the user ID, and the Result Attribute must specify the password. For OpenLDAP, use `(&(ObjectClass=inetOrgPerson)(cn=%s))` for the Query Filter, and `userPassword` for the Result Attribute.

> ***Note*** *For either method, access is refused if the LDAP server direct query or bind attempt fails for any reason, for example, an invalid user name or password, bad query, or if the LDAP server is not responding.*



LDAP Authenticated Sessions

LDAP Authenticated Sessions

Directory server: LDAP

Search Base: dc=example,dc=com

Scope: Subtree

Query Filter: (sAMAccountName=%s)

Result Attribute: mail

Timeout: 5

3. From the **Directory Server** drop-down list, select a server to perform the search.
4. In the **Search Base** text box, type a **Search Base** string with information specific to your LDAP hierarchy.

   For example: `cn=users,dc=example,dc=com`.

5. From the **Scope** drop-down list, select the scope of the search.

   - **Base** – Searches the base object only.
   - **One Level** – Searches objects beneath the base object, but excludes the base object.
   - **Subtree** – Searches the entire subtree of which the base distinguished name is the topmost object, and includes the base object.

6. In the **Query Filter** text box, type the filter for the LDAP lookup.

   For example, for Active Directory, type:`(sAMAccountName=%s)`.

   For OpenLDAP, type: `(&(ObjectClass=inetOrgPerson)(cn=%s))`. For iPlanet, type: `uid=%s`.

7. In the **Result Attribute** text box, type the attribute that returns the user's account.

   For example, for Active Directory, type: `mail`.

   For OpenLDAP, type: `userPassword`. For iPlanet, type: `mail`.

   If your organization has multiple LDAP domains, or if the domain of the WatchGuard XCS is different than the LDAP domain, then the LDAP authentication Bind method must be used for Web User authentication.

   For example, for Active Directory, the LDAP Query Filter must consist of the user name, for example, `samAccountName=%s`, and the Result Attribute should be `mail`.

   For OpenLDAP, use `cn=%s` and `mail`.

   This makes sure you properly match user, domain, and group policies for this LDAP user.

8. In the **Timeout** text box, type the maximum interval, in seconds, to wait for the search to complete.
   You can enter values from 1 to 100 seconds.
9. Click the **Test** button to perform a test of the LDAP Authentication configuration.
10. Click **Apply**.

LDAP Virtual Mappings

Use *Virtual Mappings* to accept mail addressed for one domain and redirect it to a different domain. This process is performed without modifying the To: and From: headers in the mail. Virtual mappings only modify the envelope-recipient address.

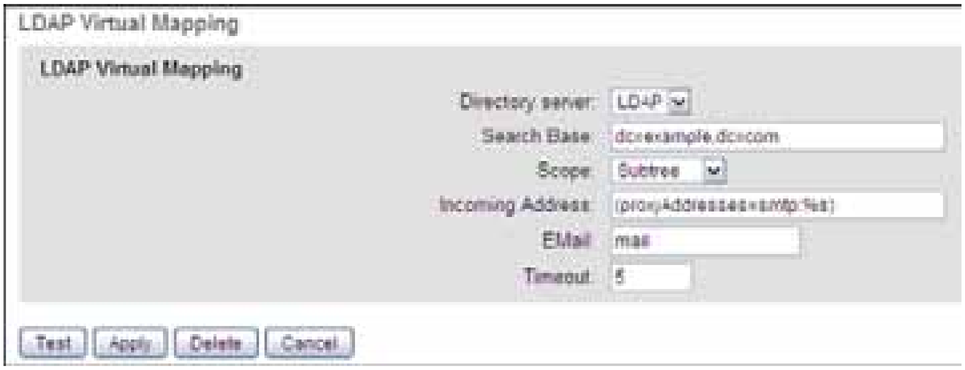
For example, you can configure the WatchGuard XCS to accept mail for the domain @example.com and deliver it to @sales.example.com. This allows you to distribute mail to multiple internal servers based on the Recipient: address of the incoming mail.

You can use LDAP mappings to search LDAP-enabled directories for user virtual mappings. See *Virtual Mappings* for more information on Virtual Mappings.

> ***Note*** *LDAP Virtual Mappings have only been tested with Active Directory, and the examples shown are for Active Directory LDAP implementations. In most cases, Active Directory already performs its own internal virtual mapping translations so configuring LDAP Virtual Mappings is not required.*

To configure LDAP Virtual Mappings:

1. Select **Configuration > LDAP > Mapping**.
   The LDAP Virtual Mapping page appears.
2. Click **Add**.



Directory server: LDAP
Search Base: dc=example,dc=com
Scope: Subtree
Incoming Address: (proxyAddresses=smtp:%s)
EMail: mail
Timeout: 5

3. From the **Directory Server** drop-down list, select a server to perform the search.
4. In the **Search Base** text box, type a **Search Base** string with information specific to your LDAP hierarchy.

   For example: `cn=users,dc=example,dc=com`.

5. From the **Scope** drop-down list, select the scope of the search.

   - **Base** – Searches the base object only.
   - **One Level** – Searches objects beneath the base object, but excludes the base object.
   - **Subtree** – Searches the entire subtree of which the base distinguished name is the topmost object, and includes the base object.

6. In the **Incoming Address** text box, type the attribute that defines the virtual mapping for a user.

   For example, for Active Directory, type:`(proxyAddresses=smtp:%s)`

7. In the **Email** text box, type the attribute that returns the user’s email address.

   For example, for Active Directory, type: `mail`

8. In the **Timeout** text box, type the maximum interval, in seconds, to wait for the search to complete.
   You can enter values from 1 to 100 seconds.
9. Click the **Test** button to perform a test of the LDAP mappings configuration.
10. Click **Apply**.

LDAP Recipients

The *LDAP Recipients* feature is used in conjunction with the Intercept Anti-Spam *Reject on Unknown Recipient* feature. Reject on Unknown Recipient must be enabled for LDAP Recipients to work properly. When a mail message is received by the system, LDAP Recipients searches an LDAP directory for the existence of a recipient’s email address. If that user address does not exist in the LDAP directory, the mail is rejected.

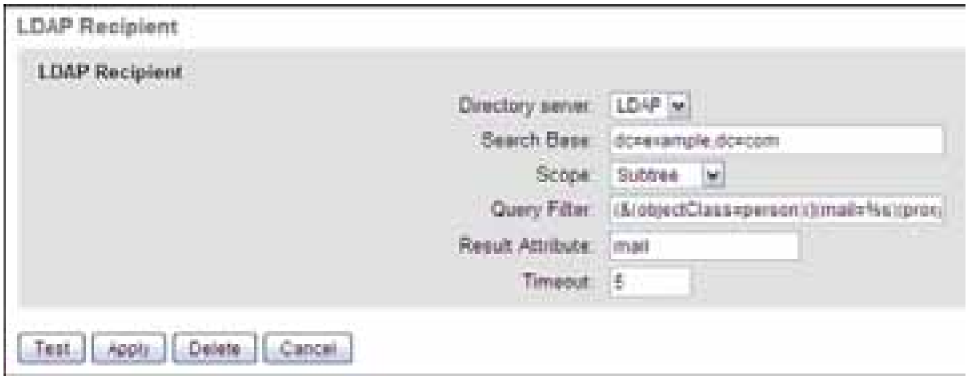
This feature differs from the LDAP Users lookup option, which searches for a user in the imported, locally-cached LDAP users database. The LDAP Recipients feature performs a direct lookup on a configured LDAP directory server for each address.

> **Note** *If you use an Active Directory server, we recommend that you use the LDAP Users feature.*

If *Reject on Unknown Recipient* is enabled for both *LDAP Users* and *LDAP Recipients*, the system checks the local and mirrored LDAP Users first, and then sends a direct query to an LDAP server.

To configure LDAP recipient lookups:

1. Select **Configuration > LDAP > Recipients**.
   The LDAP Recipient page appears.
2. Click **Add**.



LDAP Recipient

LDAP Recipient

Directory server: LDAP

Search Base: dc=example,dc=com

Scope: Subtree

Query Filter: (&(objectClass=person)(|(mail=%s)(prox

Result Attribute: mail

Timeout: 5

3. From the **Directory Server** drop-down list, select a server to perform the search.
4. In the **Search Base** text box, type a **Search Base** string with information specific to your LDAP hierarchy.

   For example: `cn=users,dc=example,dc=com`.

5. From the **Scope** drop-down list, select the scope of the search.

- **Base** – Searches the base object only.
- **One Level** – Searches objects beneath the base object, but excludes the base object.
- **Subtree** – Searches the entire subtree of which the base distinguished name is the topmost object, and includes the base object.

6. In the **Query Filter** text box, type the filter for the LDAP Recipients lookup.

   For example, for Active Directory, type:
   `(&(objectClass=person)(|(mail=%s)(proxyaddresses=SMTP:%s)))`

   For OpenLDAP and iPlanet, type: `(&(objectClass=person)(uid=%s))`
7. In the **Result Attribute** text box, type the attribute that returns the user's email address.

   For example, for Active Directory, OpenLDAP, and iPlanet, type: `mail`
8. In the **Timeout** text box, type the maximum interval, in seconds, to wait for the search to complete.
   You can enter values from 1 to 100 seconds.
9. Click the **Test** button to perform a test of the LDAP Recipients configuration.
10. Click **Apply**.

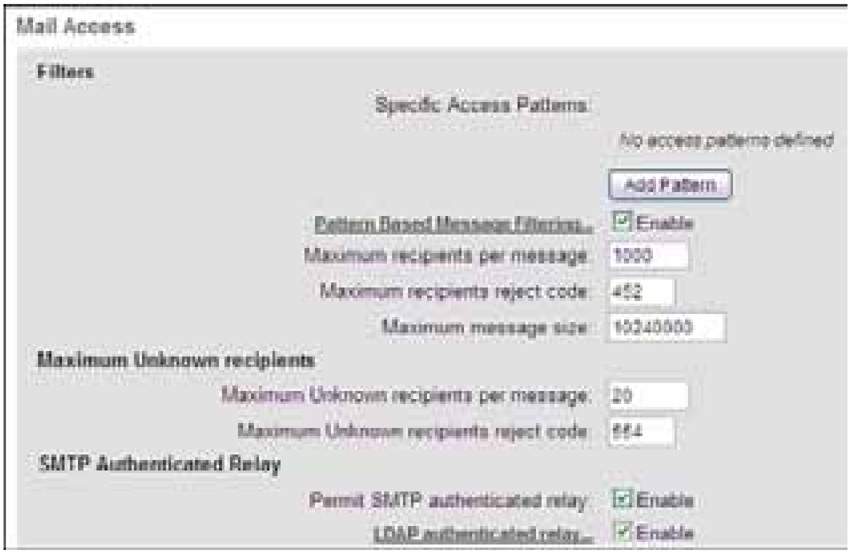
LDAP SMTP Authenticated Relay

The *LDAP SMTP Authenticated Relay* feature allows authenticated clients to use this system as an external mail relay for sending mail. For example, you may have remote users in your organization that need to send mail through this WatchGuard XCS.

These client systems must use a login and password to authenticate to the WatchGuard XCS before they are allowed to relay mail. These accounts can be set up as local accounts, but you can also use LDAP relay authentication to authenticate the user to an LDAP directory server.

To configure LDAP Authenticated SMTP Relay:

1. Select **Configuration > Mail > Mail Access**.
   The Mail Access page appears.
2. Select the **Permit SMTP Authenticated Relay** and the **LDAP Authenticated Relay** check boxes.



Mail Access

Filters

Specific Access Patterns

No access patterns defined

Pattern Based Message Filtering... ☑ Enable

Maximum recipients per message: 1000

Maximum recipients reject code: 452

Maximum message size: 10240000

Maximum Unknown recipients

Maximum Unknown recipients per message: 20

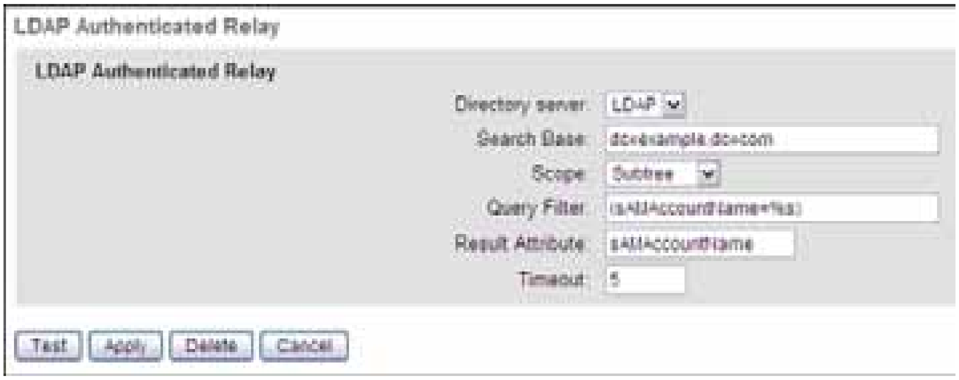
Maximum Unknown recipients reject code: 554

SMTP Authenticated Relay

Permit SMTP authenticated relay: ☑ Enable

LDAP authenticated relay... ☑ Enable

3. Select **Configuration > LDAP > Relay**.
   The LDAP Authenticated Relay page appears.



Directory server: LDAP
Search Base: dc=example,dc=com
Scope: Subtree
Query Filter: (sAMAccountName=%s)
Result Attribute: sAMAccountName
Timeout: 5

4. Select a query method for contacting the LDAP server.

   For Active Directory and iPlanet implementations, use the **Bind** method. For OpenLDAP, use the **Query Direct** method.

   - **Bind** – The Bind method uses the User ID and password to authenticate on a successful bind. The Query Filter must specify the User ID with a %s variable. For example, for Active Directory, enter `(sAMAccountName=%s)`. The Result Attribute must be a User ID, for example, `sAMAccountName`.
     For iPlanet, use `uid=%s` for Query Filter, and `mail` for Result Attribute.
   - **Query Direct** – The Query Direct method queries the LDAP server directly to authenticate a user ID and password. The Query Filter must specify the user ID, and the Result Attribute must specify the password. For OpenLDAP, use `uid=%s` for Query Filter, and `userPassword` for Result Attribute.

   For the Bind or Query Direct method, the relay is refused if the LDAP server direct query or bind attempt fails for any reason, for example, an invalid user name or password, bad query, or if the LDAP server is not responding.

5. Click **Add**.
   You can only use one method, Bind or Query Direct, for all defined LDAP servers.
6. From the **Directory Server** drop-down list, select a server to perform the search.
7. In the **Search Base** text box, type a **Search Base** string with information specific to your LDAP hierarchy.

   For example: `cn=users,dc=example,dc=com`.

8. From the **Scope** drop-down list, select the scope of the search.

   - **Base** – Searches the base object only.
   - **One Level** – Searches objects beneath the base object, but excludes the base object.
   - **Subtree** – Searches the entire subtree of which the base distinguished name is the topmost object, and includes the base object.

8. In the **Query Filter** text box, type a query for the LDAP lookup.

   For example, for Active Directory type:`(sAMAccountName=%s)`

9. In the **Result Attribute** text box, enter the attribute that returns the user’s account.

   For example, for Active Directory type: `sAMAccountName`

10. In the **Timeout** text box, type the maximum interval, in seconds, to wait for the search to complete.
    You can enter values from 1 to 100 seconds.
11. Click the **Test** button to perform a test of the LDAP relay configuration.
12. Click **Apply**.

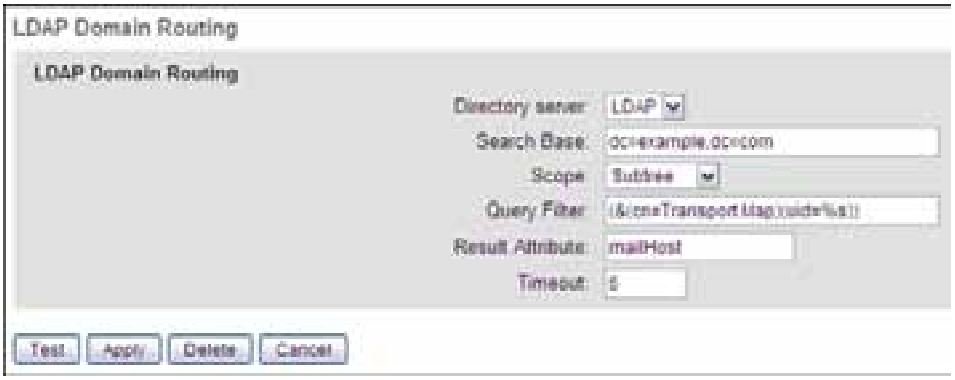
LDAP Routing

LDAP routing allows you to query for a mail route for a recipient on a specified LDAP server. The destination mail server for that domain is returned and the message is routed to that server. This is the preferred method for mail routing for organizations with a large amount of domains. Any locally defined mail routes (in **Configuration > Mail > Routing**) are resolved before LDAP routing.

> ***Note*** *LDAP routing has only been tested with iPlanet implementations but the examples provided should also work with OpenLDAP, depending on your LDAP schema.*

To configure LDAP routing:

1. Select **Configuration > LDAP > Routing**.
   The LDAP Routing page appears.
2. Click **Add**.



LDAP Domain Routing

LDAP Domain Routing

Directory server: LDAP

Search Base: dc=example,dc=com

Scope: Subtree

Query Filter: (&(cn=Transport Map)(uid=%s))

Result Attribute: mailHost

Timeout: 5

3. From the **Directory Server** drop-down list, select a server to perform the search.
4. In the **Search Base** text box, type a **Search Base** string with information specific to your LDAP hierarchy.

   For example: `cn=users,dc=example,dc=com`.

5. From the **Scope** drop-down list, select the scope of the search.

   - **Base** – Searches the base object only.
   - **One Level** – Searches objects beneath the base object, but excludes the base object.
   - **Subtree** – Searches the entire subtree of which the base distinguished name is the topmost object, and includes the base object.

6. In the **Query Filter** text box, type the query filter that searches for the Mail Domain of a recipient.

   For example, for iPlanet type:`(&(cn=Transport Map)(uid=%s))`

7. In the **Result Attribute** text box, type the attribute that returns the domain's mail host.

   For example, for iPlanet, type: `mailHost`

8. In the **Timeout** text box, type the maximum interval, in seconds, to wait for the search to complete.
   You can enter values from 1 to 100 seconds.
9. Click the **Test** button to perform a test of the LDAP routing configuration.
10. Click **Apply**.

Troubleshoot LDAP Issues

These sections describe several common LDAP problems and procedures for their resolution.

Cannot Contact the LDAP Server

This error is displayed in the logs if LDAP User imports fail:

```
Nov 16 17:03:13 server root: ldap_bind: Can't contact LDAP server (81)
```

Examine these items:

- Verify that the LDAP Server is up and running.
- In **Configuration > LDAP > Directory Servers**, verify the address of the LDAP Server.
- Make sure that LDAP or LDAPS is used properly in the LDAP server URI.
- Make sure nothing is blocking LDAP traffic for the WatchGuard XCS and the LDAP Server. For example, if the WatchGuard XCS is installed on a network off of the network firewall, make sure it can connect to the LDAP server on TCP port 389 (LDAP) or 636 (LDAPS).
- Test connectivity with the LDAP Server. Telnet to the LDAP Server on TCP port 389 or 636.

LDAP User and Group Imports are Failing

If LDAP Users and Groups are not being imported, check **Activity > Logs > System** for any of these errors:

```
Nov 19 14:14:23 hostname spl: ALARM: LDAP import: serious: Import of users failed.Nov 19
14:14:23 hostname spl: LDAP import of users failed.Nov 19 14:14:23 hostname root: ldap_
bind: Invalid credentials (49)
```

These messages indicate that the system can contact the LDAP Server, but either the user does not have the correct credentials to perform a search, or the Bind DN does not exist.

- In **Configuration > LDAP > Directory Servers**, verify that you specified the correct Bind DN.
- Verify the Bind DN is correct. The configured Bind DN user on the system is only used to search the LDAP Server. In Active Directory, this is any user in the Domain Users Group. In an Active Directory environment the DN would look like:

  ```
  cn=User name,cn=users,dc=example,dc=com
  ```

  For example:

  ```
  cn=Ken R. Simon,ou=users,dc=example,dc=com
  ```

- Verify that the user can log in to the domain. If this user cannot log in to the domain, verify the user name and password.

Mirror Accounts are Not Created

If the system is able to connect to the LDAP Server and import users, but fails to create any or only some mirrored accounts, examine these items:

- If the system is not creating mirrored users, make sure that **Mirror Accounts** is enabled in **Configuration > LDAP > Directory Users > Import Settings**.
- Verify that the search base is correct and is not too restrictive. Try re-importing with a wider search base.
- Make sure that the email attribute is set correctly in **Configuration > LDAP > Directory Users**. In most environments it is typically set to `mail`.
- Verify that users have an assigned email address. The system only creates mirrored accounts for user accounts that have an email address. In Active Directory, make sure the user has a valid email address.
- If a valid email address exists, verify that the system can view it. Click the **Test** button in **Configuration > LDAP > Directory Users**. Specify the user in the **LDAP Query Field**, for example, `(sAMAccountName=username)` and use `mail` as the attribute for the returned data.

```
# extended LDIF
#
# LDAPv3
# base with scope sub
# filter: (sAMAccountName=ksimon)
# requesting: mail
#

# Ken R. Simon, users, example.com
dn: CN=Ken R. Simon,OU=users,DC=example,DC=com
mail: ksimon@example.com
```

In the previous example, the final line indicates the mail attribute returned.

LDAP Authentication Failures

If the system is able to contact the LDAP server, but when trying to login you receive this error message “Invalid Login”, check the logs to see why the login failed in **Activity > Logs > System**.

Typically, this type of error message appears:

```
Nov 22 15:24:49 server login.spl: fail login as 'jsmith' [dom:0]: Invalid
RADIUS/LDAP login [ip:10.10.8.224]
```

Use the LDAP Test Feature in **Configuration > LDAP > Directory Users** to verify the user exists. For the LDAP Query, specify the user name attribute and the user name. For example, for Active Directory use `(sAMAccountName=jsmith)`.

If the LDAP test does not return any results from the search then it is possible that the user name is incorrect, does not exist, or the search base is too restrictive. Repeat the test with a broader search base. If the system does not find the user after performing this step, verify that the user name exists by checking the directory server itself.

If the LDAP test does find the user, the password may be incorrect or the user cannot login because either the user does not have the required permissions or the account is disabled. Verify that the user can log in to the domain.

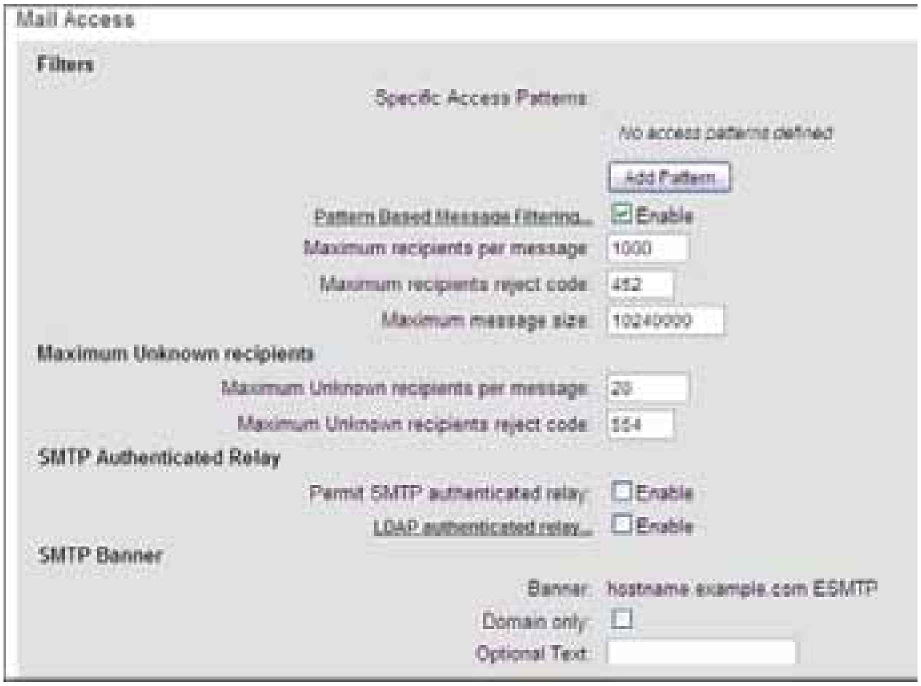
8 Mail Security

Mail Access

Use the *Mail Access* page to configure features that provide security when the WatchGuard XCS is accepting mail during an SMTP connection.

To configure your SMTP mail access settings:

1. Select **Configuration > Mail > Access**.
   The Mail Access page appears.



Mail Access

Filters

Specific Access Patterns

No access patterns defined

Pattern Based Message Filtering... ☑ Enable

Maximum recipients per message: 1000

Maximum recipients reject code: 452

Maximum message size: 10240000

Maximum Unknown recipients

Maximum Unknown recipients per message: 20

Maximum Unknown recipients reject code: 554

SMTP Authenticated Relay

Permit SMTP authenticated relay: ☐ Enable

LDAP authenticated relay... ☐ Enable

SMTP Banner

Banner: hostname.example.com ESMTP

Domain only: ☐

Optional Text:

Specific Access Patterns

Use Specific Access Patterns to search for patterns in a message for filtering during the SMTP connection. See *Specific Access Patterns* for detailed information on configuring these filters.

Pattern Based Message Filtering

Use Pattern Filters to reject or accept mail based upon matches in the message envelope, header, or body. See *Pattern Filters* for detailed information on configuring Pattern Filters.

Maximum recipients per message

Set the maximum number of recipients accepted per message. A very large amount of recipients means the message is more likely to be spam or bulk mail. The default is set to 1000.

Maximum recipients reject code

Allows administrators to define other errors to return instead of the default “452 Error: too many recipients” error, for example, permanently rejecting the connection “554”.

Maximum message size

Set the maximum message size (in bytes) that is accepted by the system. The default is 10240000 bytes. Note that processing large messages decreases mail processing performance.

The **Attachment Size Limit** option configured in **Security > Content Control > Attachment Control** is also set to 10240000 bytes, and as a result, the threshold is exceeded if the attachment size is close to the attachment size limit. We recommend that you set the **Maximum Message Size** value to at least 1.5 times the value of the **Attachment Size Limit** option. When attachments are sent with most email messages, the message size grows considerably because of the encoding methods. The maximum message size should be set accordingly to accommodate attachments. Attachments are sent base64 encoded, not in their binary form. Base64 encoding can increase the size of a file to up to 140% of its original size. A 9MB attachment is actually 13MB in size, and would exceed a message size limit of 10MB. You must consider the additional overhead caused by base64 encoding when configuring a maximum message limit.

Minimum Queue Free Space (Cluster Primary Only)

This option only appears on a Cluster Primary system and allows administrators to set the minimum amount of free space in kilobytes that is required in the queue file system to receive messages. If the system has less than the specified free space, messages are rejected with a “452: Insufficient system storage” error. This value must at minimum be greater than 1.5 times the specified **Maximum message size**, and at maximum 50 GB. The default value is automatically calculated for clusters with all the same hardware, and this configuration is replicated across all cluster systems. In a cluster that contains systems of different types of hardware, you must set this value to 20% of the total *System Data Storage Area* space available according to the cluster member with the least space. To view this information, select **Activity > Status > Utilities** on the cluster member. For example, if the cluster system with the least amount of *System Data Storage Area* space has 10 GB available, then set this value to 2097152 KB (2 GB).

Note *The Minimum Queue Free Space value is not synchronized through Centralized Management.*

Maximum Unknown recipients per message

This value determines how many unknown recipients are allowed in the message before it is rejected by the system. A high number of unknown recipients indicates the message is likely spam or a denial of service attempt.

Maximum Unknown recipients reject code

This value indicates the SMTP reject code to use when the maximum unknown recipients value is exceeded. This option can be set to “421” (temporary reject) or “554” (permanent reject).

SMTP Authenticated Relay

This feature allows authenticated clients to use the system as an external mail relay for sending mail. For example, you may have remote users who need to send mail through this system. Clients must use a login and password to authenticate to the system before they are allowed to relay mail. These accounts can be local or they can be authenticated through LDAP.

LDAP SMTP Authentication

SMTP authentication can be performed to an LDAP directory server. Select the check box to enable LDAP Authenticated Relay, and select the link to configure its options. This feature can also be configured in **Configuration > LDAP > Relay**. See *LDAP SMTP Authenticated Relay* for detailed information on configuring LDAP Authenticated Relay.

SMTP Banner

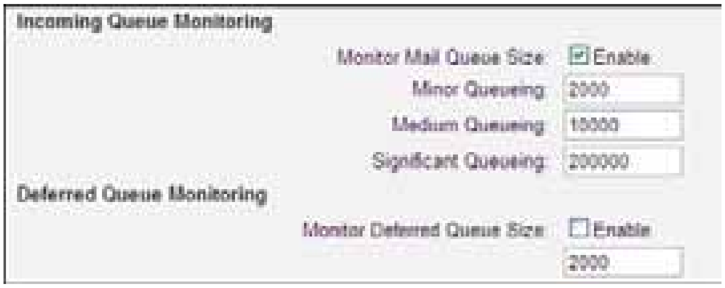
The SMTP banner is exchanged during the HELO/EHLO session of an SMTP connection.
The banner contains identifying information for your mail server that can be used as information to launch attacks against it. This option allows you to customize the SMTP banner. Select **Domain only** to remove the hostname from the banner.

Queue Monitoring

The Queue Monitoring feature allows you to modify the system’s behavior depending on the size of the incoming mail queue. To process the current mail queue faster, you can give a higher priority to the delivery of queued mail than receiving new mail when a threshold is reached.
At the maximum threshold, incoming requests are temporarily rejected to allow the queue to process current messages first.

Select the Monitor Mail Queue Size option to enable incoming queue thresholds.

- **Minor Queueing** – If the active queue size reaches the minor threshold, the system slightly increases the priority of mail delivery over mail receiving. A *Warning* alarm is generated.
- **Medium Queueing** – If the active queue size reaches the medium threshold, the system significantly increases priority of mail delivery over mail receiving. A *Serious* alarm is generated.
- **Significant Queueing** – If the active queue size reaches the significant threshold, the system temporarily rejects any new mail and notifies the administrator. A *Critical* alarm is generated.



Incoming Queue Monitoring

Monitor Mail Queue Size: ☑ Enable

Minor Queueing: 2000

Medium Queueing: 10000

Significant Queueing: 200000

Deferred Queue Monitoring

Monitor Deferred Queue Size: □ Enable

2000

Deferred Mail Queue Size monitoring

This feature monitors the size of the deferred mail queue and generates a critical alarm if the deferred queue size threshold is exceeded. Your deferred mail queue can grow in size if your XCS device experiences issues with outbound mail.

- **Monitor Deferred Queue Size** – Select the **Enable** check box to monitor the deferred mail queue.
- **Threshold** – Indicates the threshold size for the deferred mail queue. A *Critical* alarm is generated if this threshold is exceeded. The default is 2000.

2. Click **Apply**.

Specific Access Patterns

Specific Access Patterns are enabled by default and can be used to accept or reject mail during an SMTP connection. Specific Access Patterns occur are processed before any other security or content processing. Use access patterns to allow email where it would be otherwise blocked, or to block email when it would otherwise be allowed. Specific access patterns allow you to respond to these local filtering requirements:

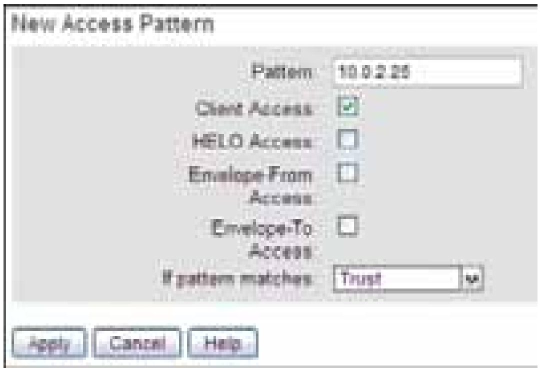
- Allow other systems to relay mail through the system
- Reject all messages from specific systems
- Allow all messages from specific systems (effectively trusting the server)

When you specify a Specific Access Pattern rule, it can take one of these forms:

- **IP Address** – The system matches the IP address, for example, 192.168.1.10, or you can use a more general address form, for example, 192.168 that matches anything in that address space. For the **Client Access** parameter, you can also use CIDR (Classless Inter-Domain Routing) format to specify a pattern for a network, for example, 192.168.0.0/24.
- **Domain Name** – The system matches the supplied domain name, for example, example.com, with any subdomain, for example, mail.example.com, and sales.mail.example.com.
- **Address** – The system matches an exact email address, for example, user@example.com, or a more general rule, for example, @example.com.

To configure a Specific Access Pattern:

1. Select **Configuration > Mail > Access**.
   The Mail Access page appears.
2. Click **Add Pattern**.
   The New Access Pattern page appears.



New Access Pattern

Pattern: 10.0.2.25

Client Access: ☑

HELO Access: ☐

Envelope-From Access: ☐

Envelope-To Access: ☐

If pattern matches: Trust

3. In the **Pattern** text box, type a mail address, IP address, hostname, or domain name.
   - **Client Access** – Specify a domain, server hostname, or IP address. This item is the most reliable and can be used to block spam and trust clients.
   - **HELO Access** – Specify a domain or server name.
   - **Envelope-From Access** – Specify a valid email address.
   - **Envelope-To Access** – Specify a valid email address.

> ***Note*** *Only the Client Access parameter is reliable because spammers can easily forge all other message properties. These parameters are useful for trusting purposes.*

4. From the **If pattern matches** drop-down list, select an action to perform:
   - **Reject** – The connection is rejected.
   - **Allow Relaying** – When you specify Allow Relaying:
     - Messages from the specified address are accepted for processing by the system
     - Messages are checked by all features. This includes Anti-Virus, Content Control, Anti-Spam, Reputation Enabled Defense, and DNSBL (DNS Block List) features
     - Messages are not checked by the Reject on Unknown Recipient feature
     - Messages can be relayed externally
   - **Trust** – The Trust option treats the server or message as part of the trusted network. When you specify the Trust action:
     - Messages from the specified address are accepted for processing by the system
     - Messages are checked by the Anti-Virus and Content Control features
     - Messages are not checked by the Anti-Spam features
     - Messages are not checked by the Reject on Unknown Recipient feature
     - Messages are not checked by the Reputation Enabled Defense and DNSBL (DNS Block List) features
     - Messages can be relayed externally
5. Click **Apply**.

Anti-Virus

The Anti-Virus scanning feature scans all messages (inbound and outbound) passing through the system for viruses. The WatchGuard XCS integrates the Kaspersky Anti-Virus engine which is one of the highest rated virus scanning technologies in the world. Anti-Virus scanning is tightly integrated with the message processing engine for maximum efficiency.

You can selectively block viruses based on whether they are found in inbound or outbound messages. Attachments are recursively disassembled to make sure that viruses cannot be concealed. When you receive a virus-infected message, you can reject, discard, or quarantine the message. You can view, download, or delete quarantined messages from the administrative quarantine area.

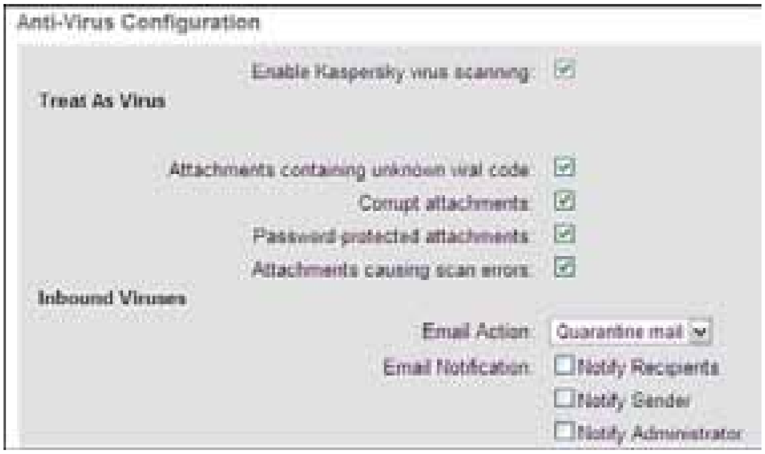
By default, if the WatchGuard XCS cannot open and examine message attachments because of password-protection, the messages are quarantined. This feature prevents password-protected zip files that contain viruses or worms from passing through the system.

Virus pattern files are automatically downloaded at regular intervals to make sure that they are always up to date. Notification messages can be sent to the sender, recipient, and administrator when an infected message is received.

McAfee Anti-Virus is also available as an add-on subscription for customers who want to enable multi-layered Anti-Virus protection.

To configure Anti-Virus scanning:

1. Select **Security > Anti-Virus > Anti-Virus**.
   The Anti-Virus Configuration page appears.



Anti-Virus Configuration

Enable Kaspersky virus scanning: ☑

Treat As Virus

Attachments containing unknown viral code: ☑
Corrupt attachments: ☑
Password-protected attachments: ☑
Attachments causing scan errors: ☑

Inbound Viruses

Email Action: Quarantine mail
Email Notification: □ Notify Recipients
□ Notify Sender
□ Notify Administrator

2. Select the **Enable Kaspersky virus scanning** check box.
3. In the **Treat as a Virus** section, you can select these options:

   Attachments containing unknown viral code

   The Anti-Virus scanner can detect code that resembles the patterns of a virus. We strongly recommend that you treat attachments containing suspected viral code as if they contained viruses.

   Corrupt attachments

   The Anti-Virus scanner may not be able to scan corrupted attachments which can contain viruses. We strongly recommend that you treat corrupt attachments as if they contained viruses.

   Password-protected attachments

Attachments protected by a password cannot be opened by the Anti-Virus scanner and could contain viruses.

> **Note** *Disable this option if you use password-protected files and archives in your organization.*

Attachments causing scan errors

Attachments that cause errors while being scanned by the Anti-Virus scanner can contain viruses. We strongly recommend that you treat attachments that cause scanning errors as if they contained viruses.

4. For both inbound and outbound mail, from the **Email Action** drop-down list, select an action to perform:

   - **Just log** – Log the event and take no further action.
   - **Reject mail** – Reject the message with notification to the sending system.
   - **Quarantine mail** – Place the message into the administrative quarantine area. This is the default action.
   - **Discard mail** – Discard the message without notification to the sending system.

5. Select the notifications to send when a virus is detected in a message.

   You can send notifications to the **Sender**, **Recipient**, and **Administrator**, and customize the notification text.

> **Note** *Variables, for example, %HOSTNAME% are inserted by the system. See System Variables for Annotations and Notifications for a full list of system variables that can be used in the notification.*

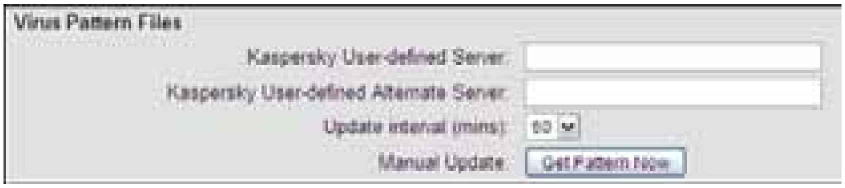
Update Pattern Files

Virus pattern files must be continuously updated to make sure that you are protected from new virus threats. The frequency of virus pattern file updates is configured in the **Virus Pattern Files** section. The WatchGuard XCS can automatically contact a default update server to update the pattern files at the specified time.

> **Note** *If you access the Internet through a proxy server, you must enter its hostname and port number in the external proxy configuration in **Configuration > Network > External Proxy Server** for pattern file updates to succeed.*

You can also define alternate sites to retrieve the Anti-Virus pattern update files from an internal location before you obtain them from external sites. You can specify up to two user-defined update servers.

The primary and alternate user-defined servers are queried in order. If the primary server cannot be contacted, the system attempts to retrieve the update from the alternate server. If the user-defined fields are not configured, the system default servers are used to retrieve the updates from external sites.



Virus Pattern Files

Kaspersky User-defined Server:

Kaspersky User-defined Alternate Server:

Update interval (mins): 60

Manual Update: Get Pattern Now

To configure virus pattern files:

1. In the **Kaspersky User-Defined Server** text box, type an optional URL that indicates the hostname and directory of the primary web server hosting the pattern file.

   Use this format:

   `http://<host>/<pathname>`
2. In the **Kaspersky User-Defined Alternate Server** text box, type an optional URL that indicates the hostname and directory of the alternate web server hosting the pattern file.
   We recommend that you use the alternate server as the default system update server.
3. From the **Update interval** drop-down list, select the interval for how often to check for pattern file updates.

   You can select **30 min**, **1 hour**, and **3 hours**. The default is 1 hour.
4. Click **Apply**.
5. Click **Get Pattern Now** to update the pattern files immediately.

   The **Kaspersky Anti-Virus Status** field displays the date and time of the last pattern file update.

Spyware Detection

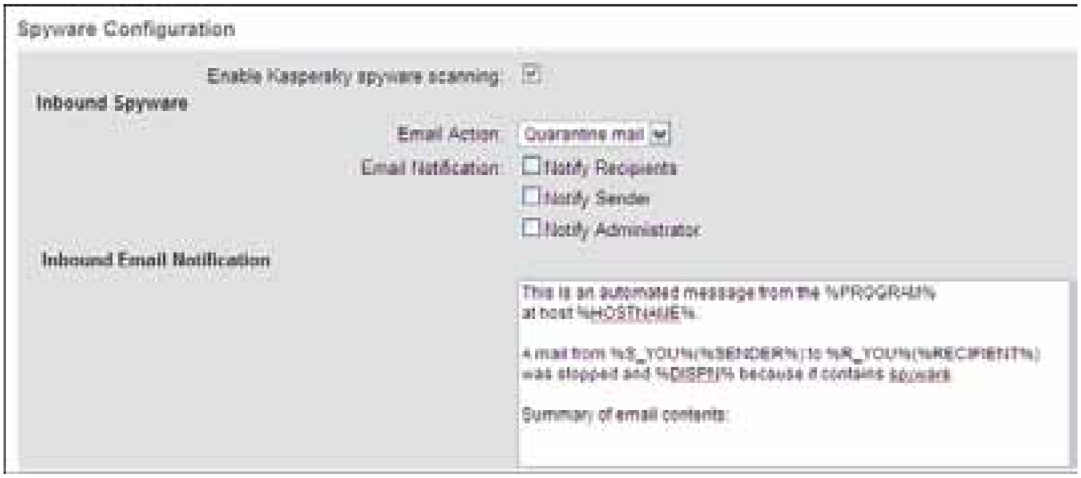
The Kaspersky Anti-Virus scanner can detect specific spyware and malware threats in addition to Anti-Virus scanning for inbound and outbound email messages and web requests.

You can enable or disable spyware detection globally and through policies. You can configure specific protocol scanning (email and web), actions, and notifications for spyware detection that are independent from the configuration of the global Anti-Virus scanner.

> ***Note*** *The Spyware action is performed after any applicable Anti-Virus action.*

To configure spyware detection:

1. Make sure Kaspersky Anti-Virus is enabled in **Security > Anti-Virus > Anti-Virus**.
   Spyware cannot be enabled and configured until Kaspersky Anti-Virus is enabled.
2. Select **Security > Anti-Virus > Spyware**.
   The Spyware Configuration page appears.



Spyware Configuration

Enable Kaspersky spyware scanning: ☑

Inbound Spyware

Email Action: Quarantine mail

Email Notification: □ Notify Recipients
□ Notify Sender
□ Notify Administrator

Inbound Email Notification

This is an automated message from the %PROGRAM%
at host %HOSTNAME%.

A mail from %S_YOU%(%SENDER%) to %R_YOU%(%RECIPIENT%)
was stopped and %DISP1% because it contains spyware.

Summary of email contents:

3. Select the **Enable Kaspersky spyware scanning** check box.
4. For both inbound and outbound email, from the **Email Action** drop-down list, select an action to perform:

   - **Just log** – Log the event and take no further action.
   - **Reject mail** – Reject the message with notification to the sending system.
   - **Quarantine mail** – Place the message into the administrative quarantine area. This is the default action.
   - **Discard mail** – Discard the message without notification to the sending system.

5. Select the notifications to send when spyware is detected in a message.

   You can send notifications to the **Sender**, **Recipient**, and **Administrator**, and customize the notification text.

> **Note** *Spyware actions for web requests must be set in a policy. You can set email spyware actions globally and within a policy.*

Outbreak Control

The *Outbreak Control* feature provides you with zero-day protection against early virus outbreaks. For most virus attacks, it can be several hours from the moment the virus is released to the time a pattern file is available. During this period, mail recipients are vulnerable to potential threats.

Outbreak Control detects early virus outbreaks and takes immediate action contain the virus threat. If a message is classified as containing a possible virus, you can quarantine or discard message. When the WatchGuard XCS receives an updated Anti-Virus pattern file, any quarantined files are re-scanned automatically. If a virus is detected with the new pattern file, the configured Anti-Virus action is performed on the message. If the hold period for a message in the quarantine expires and the message has not been positively identified as a virus during that time, the configured “release” action is performed.

The WatchGuard XCS examines incoming untrusted messages and looks for these characteristics when deciding if the message indicates an early virus threat:

- The message originates from an IP address that has recently sent viruses and the message contains an executable or common office document attachment. To detect if the client has recently sent viruses, you must enable the Mail Anomalies feature and the **Recent virus from Client** option.

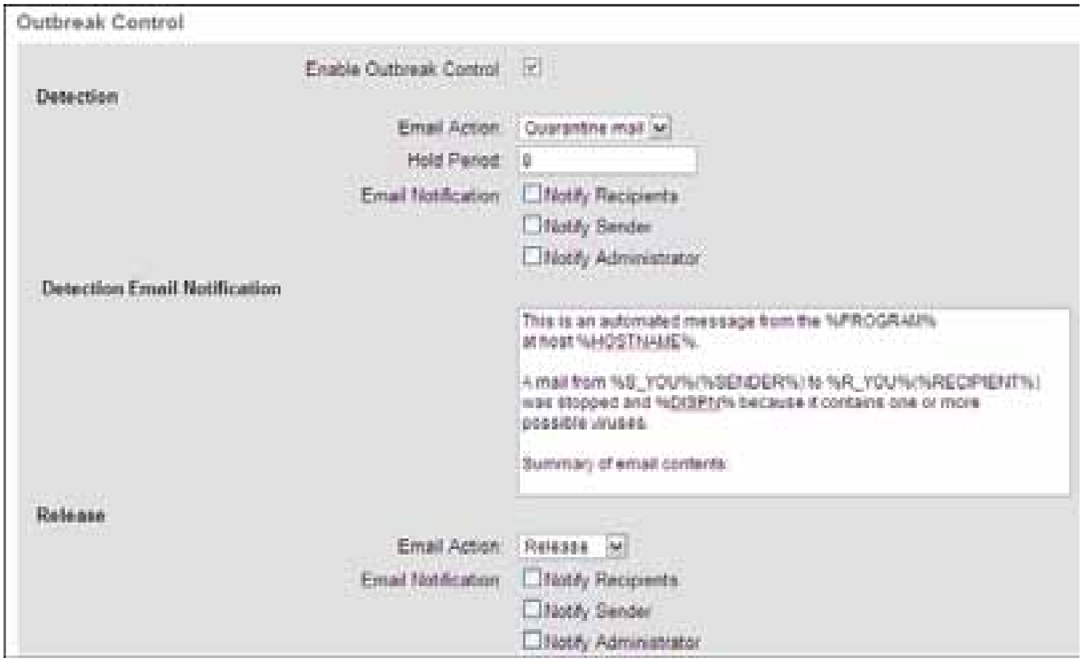
- The message originates from an IP address with a poor reputation and the message contains an executable or common office document attachment. To detect addresses with a poor reputation, you must enable the Reputation Enabled Defense feature.
- The Anti-Virusscanner detectsattachments thatresemble aknown virusor containunknown viralcode.

This table lists the types of executable files and common office document formats that are scanned by Outbreak Control:.

Executable	Common Office Documents
bat	.doc
.chm	.dot
.cmd	.ppt
.com	.wk1
.dll	.wks
.drv	.wp
.exe	.xls
.js	
.jse	
.nlm	
.ovl	
.pif	
.scr	
.shs	
.sys	
.vbe	
.vbs	
.vxd	

To configure Outbreak Control:

1. Select **Security > Anti-Virus > Outbreak Control**.
   The Outbreak Control page appears.



Outbreak Control

Enable Outbreak Control ☑

Detection

Email Action: Quarantine mail

Hold Period: 8

Email Notification: □ Notify Recipients □ Notify Sender □ Notify Administrator

Detection Email Notification

This is an automated message from the %PROGRAM%
at host %HOSTNAME%.

A mail from %S_YOU%(%SENDER%) to %R_YOU%(%RECIPIENT%)
was stopped and %DISP%% because it contains one or more
possible viruses.

Summary of email contents:

Release

Email Action: Release

Email Notification: □ Notify Recipients □ Notify Sender □ Notify Administrator

2. From the **Email Action** drop-down list, select an action to perform if a possible virus is detected.

   - **Just Log** – The message is delivered to its destination and an entry added to the mail log.
   - **Reject mail** – Reject the message with notification to the sender.
   - **Quarantine mail** – Place the message into the administrative quarantine area. This is the default action.
   - **Discard mail** – Discard the message without notification to the sender.

3. In the **Hold Period** text box, type the time (in hours) for which to hold the message in the administrative quarantine area.

   The default hold period is 8 hours. In most cases, the Anti-Virus pattern files are updated within 2-4 hours of the discovery of a new virus. We recommend that you configure enough time to allow the opportunity for the files to be rescanned with updated Anti-Virus pattern files as they become available. If the Quarantine expiration period is set to a value less than the **Hold Period**, the expiry period takes precedence and the quarantined message is expired.

   During the hold period, if a quarantined message is rescanned and determined to have a virus, the configured Anti-Virus action is performed as set in **Security > Anti-Virus > Anti-Virus**. If the hold period expires and the message is determined not to be infected with a virus, the **Release** action is performed.

4. Select the notifications to send when a suspicious message is detected by Outbreak Control.

   You can send notifications to the **Sender**, **Recipient**, and **Administrator**, and customize the notification text

5. In the **Release** section, from the **Email Action** drop-down list, select an action to perform if the **Hold Period** expires for a quarantined message:

   - **Just Notify** – A notification is sent to the specified users that the **Hold Period** for a quarantined message has elapsed without the message being classified as a virus. The message remains in the quarantine until you release the message manually.

- **Release mail** – The message is automatically released from the quarantine and delivered to the original recipients.

6. Select the notifications to send when a message is released from the quarantine.

   You can send notifications to the **Sender**, **Recipient**, and **Administrator**, and customize the notification text.

> ***Note*** *To search for the disposition of messages caught by Outbreak Control in **Activity > History > Message History**, search for a subject that contains "possible virus".*

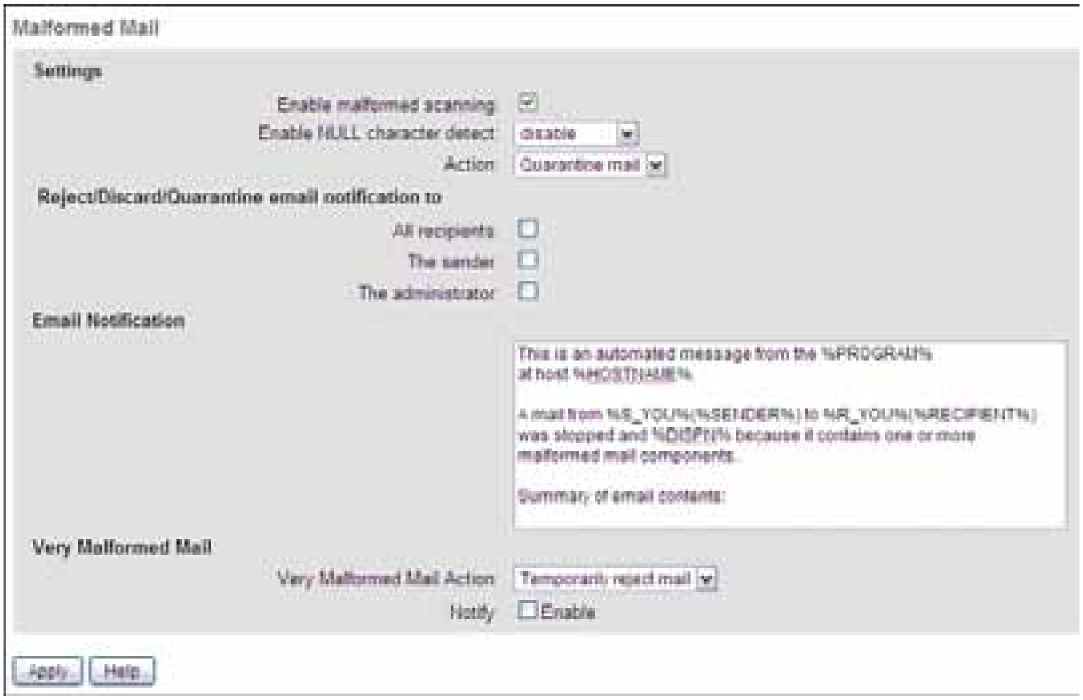
Malformed Mail

Many viruses try to elude virus scanners by concealing themselves in malformed messages. The scan engines cannot detect the attachment and pass the complete message through to an internal server. Some mail clients try to rebuild malformed messages and can rebuild or activate a virus-infected attachment. Other types of malformed messages are designed to attack mail servers directly. These types of messages are typically used in denial-of-service (DoS) attacks.

The system analyzes each message with extensive integrity checks. You can quarantine malformed messages if they cannot be processed.

To configure malformed mail scanning:

1. Select **Security > Anti-Virus > Malformed Mail**.
   The Malformed Mail page appears.



Malformed Mail

Settings

Enable malformed scanning ☑

Enable NULL character detect: disable

Action: Quarantine mail

Reject/Discard/Quarantine email notification to

All recipients ☐

The sender ☐

The administrator ☐

Email Notification

This is an automated message from the %PROGRAM%
at host %HOSTNAME%.

A mail from %S_YOU%(%SENDER%) to %R_YOU%(%RECIPIENT%)
was stopped and %DISP%% because it contains one or more
malformed mail components.

Summary of email contents:

Very Malformed Mail

Very Malformed Mail Action: Temporarily reject mail

Notify ☐ Enable

2. Select the **Enable malformed scanning** check box.
3. From the **Enable NULL character detect** drop-down list, select **Enable** to consider messages containing null characters (a byte value of 0) in the raw mail body as a malformed message.

   NULL character detect is disabled by default.

   > **Note** *The null character detection feature can cause incompatibility with certain mail servers and we recommend that you disable this feature if issues occur.*

4. From the **Action** drop-down list, select an action to perform when a malformed message is detected.

   - **Just log** – Log the event and take no further action.
   - **Reject mail** – Reject the message with notification to the sending system.
   - **Quarantine mail** – Place the message into the administrative quarantine area. This is the default action.
   - **Discard mail** – Discard the message without notification to the sending system.

5. Select the notifications to send when a malformed message is detected.

   You can send notifications to the **Sender**, **Recipient**, and **Administrator**, and customize the notification text

6. From the **Very Malformed Mail Action** drop-down list, select an action to perform when a very malformed message is detected.

   A very malformed message can cause scanning engine latency.

   - **Just log** – Log the event and take no further action.
   - **Quarantine mail** – Place the message into the administrative quarantine area.
   - **Temporarily Reject Mail** – Return an error to the sending server and do not accept the mail. The mail delivery is attempted again at a later time.
   - **Reject mail** – Reject the message with notification to the sending system.
   - **Discard mail** – Discard the message without notification to the sending system.

7. Select the **Notify** check box to send notifications according to the malformed notification settings (configured in **Security > Anti-Virus > Malformed Mail**) when any action except for **Just Log** is performed.

   > **Note** *Messages that are very malformed are not virus scanned or filtered for attachments and spam.*

SecureMail Email Encryption

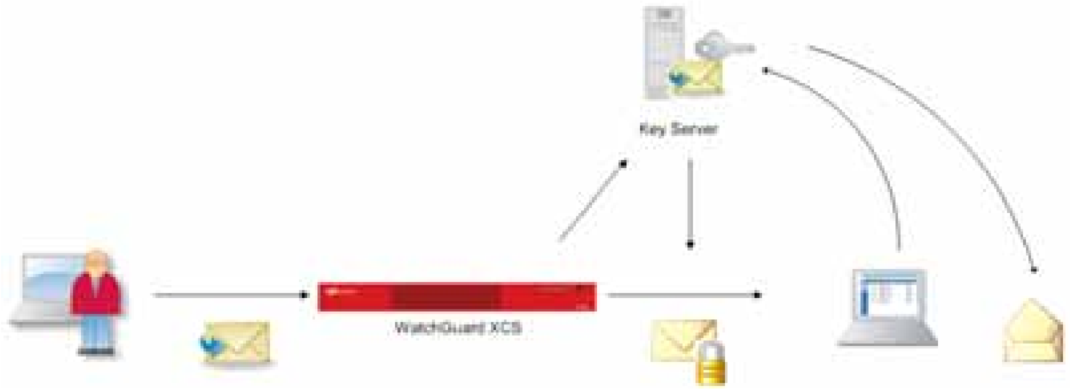
SecureMail Email Encryption allows end users to encrypt outbound messages directly from the WatchGuard XCS without the need for a local encryption server or additional desktop software. Messages are secured until they are delivered and decrypted by the recipient of the message. Recipients open an attachment to the encrypted message that allows them to create an account on the SecureMail web site and log in to read the message.

When encryption is enabled, you can use these features to scan for specific patterns in email messages that indicate the message must be encrypted.

- Pattern Filters
- Objectionable Content Filter
- Content Scanning
- Content Rules
- Document Fingerprinting

For example, you can create a Pattern Filter to search for the word "[Encrypt]" in the subject field of a message. An end user can add this phrase to their message subject header to indicate the message must be encrypted before it is delivered.

How SecureMail Email Encryption Works



1. When a user sends a message, the WatchGuard XCS uses pattern and content filters to determine if a specific encryption policy applies to the message.
2. The SecureMail engine communicates with the SecureMail service to generate encryption keys, any branding data, and creates the notification message. SecureMail uses IBE (Identity-Based Encryption) which generates encryption keys based on the sender and recipient email addresses.
3. The message is signed with the sender's public key and delivered to the recipient as a message attachment.
4. The recipient opens the attachment that allows them to register (if this is the first encrypted message received) and authenticate their email address to the SecureMail web site.
5. The SecureMail web site uses the recipient's private session key to allow the recipient to read the unencrypted message.

> **Note** *The WatchGuard XCS uses TCP port 443 (HTTPS) to communicate with the SecureMail key server. Make sure this port is correctly configured on your network firewall to allow access from the WatchGuard XCS.*

SecureMail Service

The SecureMail service allows you to send secure, encrypted messages directly to a recipient's inbox. The WatchGuard XCS integrates the encryption engine to allow messages to be encrypted on the system before it is delivered to the intended recipient. The recipient does not require any additional software or configuration to decrypt and read the message. The SecureMail architecture allows the integrated encryption engine software on the WatchGuard XCS to perform the message encryption and message delivery functions directly on your appliance, while the SecureMail service performs all encryption key-related services and provisioning.

These features are available when using the SecureMail Email Encryption service:

- **Platform independent** – You can open messages encrypted by SecureMail from any email platform, on any operating system and web browser.
- **Secure** – The secure email is encrypted with the equivalence of a 1024-bit key. Each message is also signed by the sender to ensure authenticity of the sender and data integrity of the message. In addition, all decrypted email messages are viewed through your web browser using an SSL/TLS connection.
- **Branding** – As a future enhancement, you can purchase optional SecureMail branding services to display your organization's logo and branding text on all encrypted messages.
- **Encrypted replies** – Recipients can securely reply to or forward encrypted messages they receive using the same web-based service that allows them to read the encrypted message.

License and Activate SecureMail

When you purchase SecureMail Email Encryption, you must activate the subscription from the LiveSecurity activation page.

1. From the WatchGuard Support page, select **Activate a Product**.
2. Log in, select your XCS product, then enter your activation key for SecureMail Email Encryption.
3. You must provide this information about your organization:

   - **Email Domains** – The email domains from which your users will send encrypted messages (example.com, example1.com, etc.)
   - **Gateway IP addresses** – The public IP addresses from which your WatchGuard XCS device connects to the SecureMail servers. This is required to authorize only your organization's IP addresses to establish a connection with the SecureMail service.
   - **Authorization Code** – Authorizes SecureMail Email Encryption for use with your WatchGuard XCS device. This code is entered in your SecureMail configuration on the WatchGuard XCS. The Authorization Code must be 15-20 alphanumeric characters in length and cannot contain symbols or spaces.

4. You will receive your SecureMail account information and confirmation from WatchGuard customer care in 24-36 hours.

Branding Option

A future enhancement will allow you to purchase a SecureMail branding option that can display your organization's logo and branding text on all encrypted messages.

You must provide these items:

- **Logo** – You can upload a custom logo that is displayed on encrypted message envelopes. The logo must be 370 pixels wide and 70 pixels high on a transparent background in gif, jpg or png format.

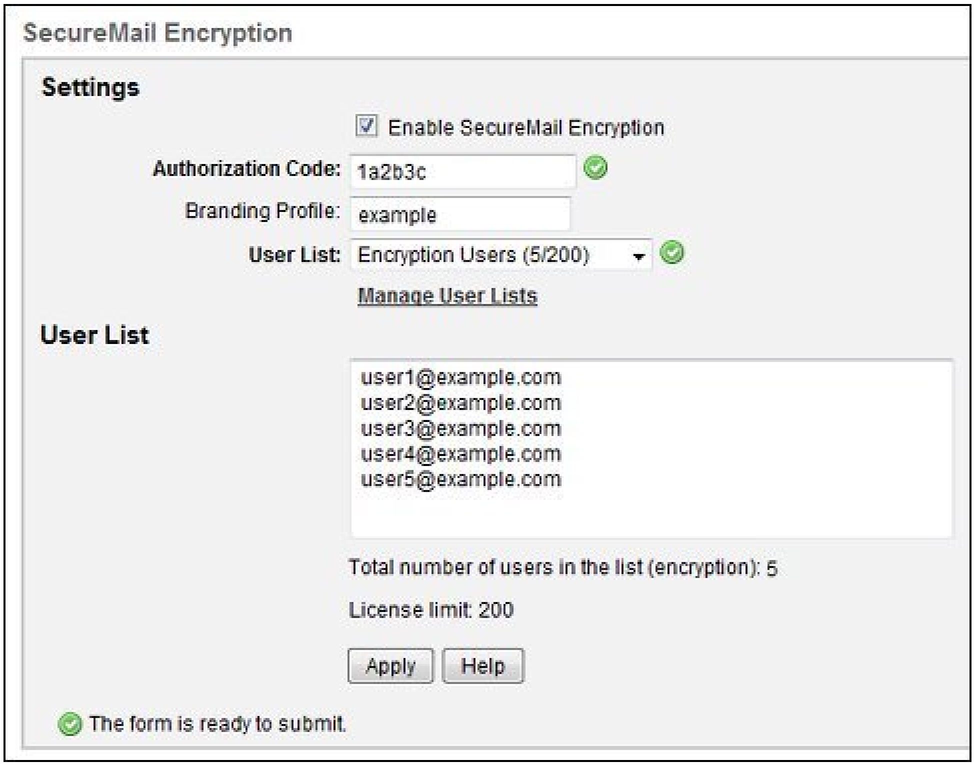
- **Branding Profile** – This value identifies your branding profile (logo and branding text) on the SecureMail service. This branding profile is entered in your SecureMail configuration on the WatchGuard XCS. The branding profile can be up to 20 alphanumeric characters, must start with a letter, and cannot contain symbols or spaces.

Configure SecureMail on the WatchGuard XCS

To configure SecureMail Email Encryption:

> ***Note*** *Make sure you have an NTP server configured in your network settings. SecureMail requires that your XCS device clock be properly set to provide accurate timestamps for the encryption process.*

1. Select **Security > Encryption > SecureMail**.
   The SecureMail Encryption page appears.



SecureMail Encryption

Settings

☑ Enable SecureMail Encryption

Authorization Code: 1a2b3c

Branding Profile: example

User List: Encryption Users (5/200)

Manage User Lists

User List

user1@example.com
user2@example.com
user3@example.com
user4@example.com
user5@example.com

Total number of users in the list (encryption): 5

License limit: 200

The form is ready to submit.

2. Select the **Enable SecureMail Encryption** check box.
3. In the **Authorization Code** text box, you must type your authorization code to authorize SecureMail Email Encryption for use with this WatchGuard device.
   You must enter an authorization code before you can enable SecureMail Email Encryption.
4. In the **Branding Profile** text box, type an optional branding profile value that corresponds to your branding profile configured with the SecureMail service.
   If you type an incorrect Branding Profile value, the default WatchGuard branding appears on the encrypted message envelope.

   This field is only required if you have purchased the Branding option for your SecureMail subscription.

5. From the **User List** drop-down list, select the list that contains the users allowed to use SecureMail encryption.
   You must upload a list of user email addresses that are permitted to encrypt messages with SecureMail encryption. If the user does not appear in the list, the message is rejected.

> ***Note*** *Only email list types that do not exceed the licensed user count appear in the drop-down list.*

6. Click **Manage User Lists** to configure and upload these lists on the Dictionaries & Lists page.
   - You must upload your list of users as an "email" list type. See *Upload User List* for details on uploading a user list.
   - The users from your file are listed in the text box, and the **Total number of users in the list** is displayed.
   - The **License Limit** indicates the maximum amount of users allowed with your license.

> ***Note*** *You cannot use email aliases with SecureMail Email Encryption.*

7. Click **Apply**.

Troubleshoot Configuration Issues

When you apply the SecureMail configuration, the WatchGuard XCS connects to the SecureMail server and tests your configuration.

If you receive an error that the WatchGuard XCS cannot contact the SecureMail server, check the following:

- The WatchGuard XCS requires an outbound HTTPS connection on port 443 to connect to the SecureMail server. Make sure this connection is allowed by your network firewall.
- The SecureMail service returns an XML-based configuration file. Make sure your network firewall or content filter allows XML files.

If the connection to the SecureMail server completes, but you receive an error that the Message Encryption verification test failed, check the following:

- Confirm that you correctly entered your Authorization Code.
- Check the gateway IP addresses you activated with SecureMail to make sure you are connecting from the public IP address of the WatchGuard XCS.

> ***Note*** *SecureMail will only encrypt messages that originate from a trusted network (outbound mail). Clients that relay mail via the WatchGuard XCS from an untrusted network and attempt to encrypt messages will be rejected.*

Upload User List

You must upload a list of user email addresses that are permitted to encrypt messages with SecureMail encryption. If the user does not appear in the list, the message is rejected with the error code "550 Error: content rejected".

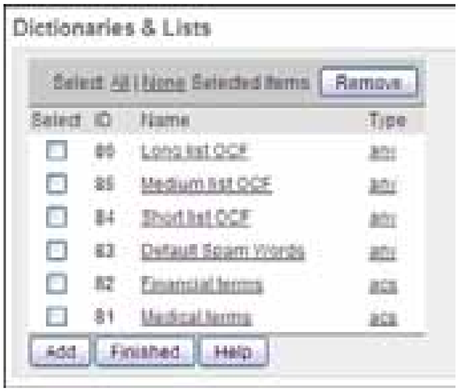
1. Create a text file containing a list of user email addresses with one address per line.

   For example:

```
user1@example.com
user2@example.com
user3@example.com
user4@example.com
user5@example.com
```

2. Click **Manage User Lists**.

   You can also select **Security > Content Control > Dictionaries & Lists** on the menu.

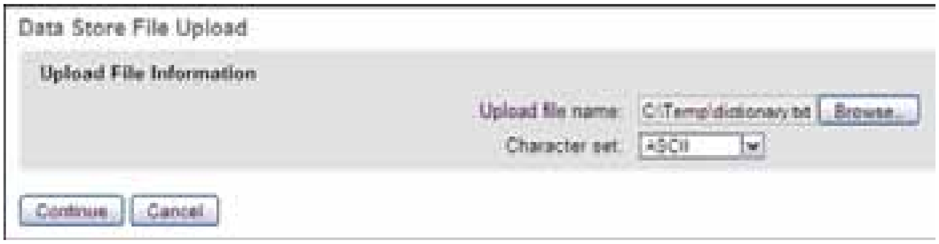


Dictionaries & Lists

Select All | None Selected items [Remove]

Select	ID	Name	Type
□	86	Long list OCF	any
□	85	Medium list OCF	any
□	84	Short list OCF	any
□	83	Default Spam Words	any
□	82	Financial terms	acs
□	81	Medical terms	acs

3. Click **Add**.



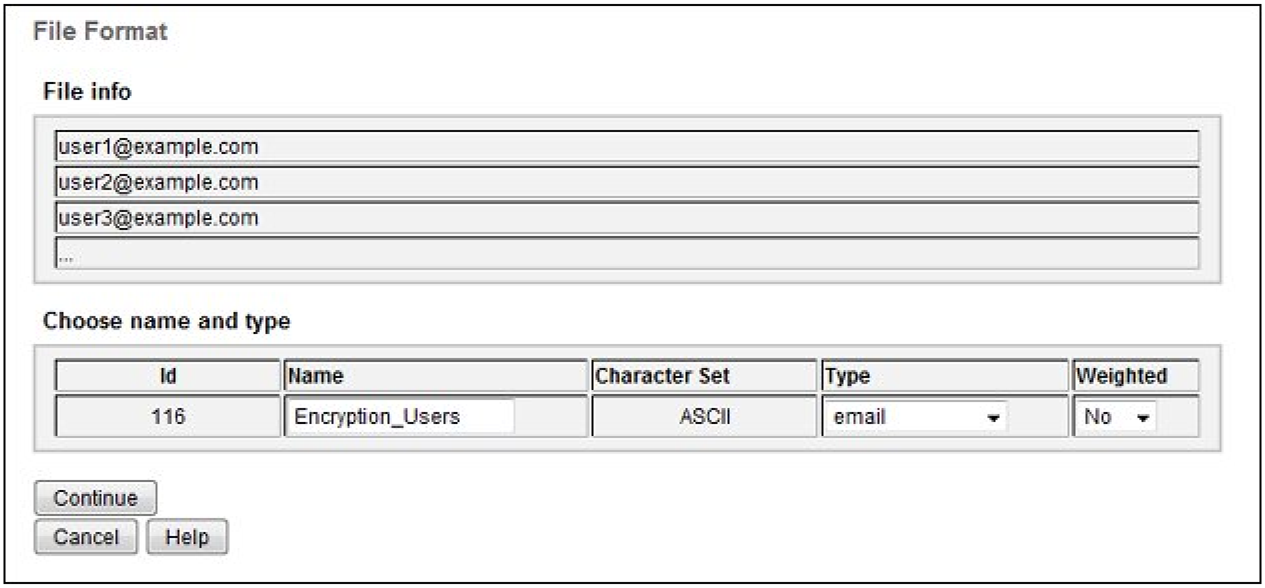
Data Store File Upload

Upload File Information

Upload file name: C:\Temp\dictionary.txt

Character set: ASCII

4. Click **Browse** to select the list of users to upload.
5. From the **Character set** drop-down list, select the encoding used in the uploaded file. For example, **ASCII**.
6. Click **Continue**.



File Format

File info

user1@example.com
user2@example.com
user3@example.com
...

Choose name and type

Id	Name	Character Set	Type	Weighted
116	Encryption_Users	ASCII	email	No

7. In the **Name** text box, type a descriptive name for the list.
8. From the **Type** drop-down list, select **email**.
9. Click **Continue** to finish uploading the file.
10. Click **Save** to save the list.

Encrypt Messages with Pattern Filters

You can create Pattern Filters to search for text in an outgoing message that identifies it as a message to be encrypted. For example, you can create a filter to search for the text “Encrypt” in a subject header to indicate the message must be encrypted before it is sent to its destination.

To configure a Pattern Filter:

1. Select **Security > Content Control > Pattern Filters**.
2. Click **Add**.
3. Create an outbound filter that searches for the word “[Encrypt]” in the subject of a message.
4. From the **Action** drop-down list, select **SecureMail Encrypt**.
   Any outbound message with the word “[Encrypt]” in the subject is encrypted before delivery.

> ***Note*** *If SecureMail is disabled globally, messages are delivered unencrypted when triggered by a Pattern Filter. Messages are rejected if you use Content Rules, OCF, Content Scanning, and Document Fingerprinting and SecureMail is disabled.*

Encrypt Messages with Content Rules

You can create Content Rules to search for text in an outgoing message that identifies it as a message to be encrypted. For example, you can create a rule to search for the text “Encrypt” in a subject header to indicate the message must be encrypted before it is sent to its destination.

To configure a Content Rule:

1. Select **Security > Content Control > Content Rules**.
2. Select the **Enable Content Rules** check box.
3. Click **Apply**.
4. Click **Outbound Content Rules**.
5. Click **Create New Rule**.
6. Create a rule that searches for the word “[Encrypt]” in the subject of a message.
7. From the **Then** drop-down list, select **SecureMail Encrypt**.
   Any outbound message with the word “[Encrypt]” in the subject is encrypted before delivery.
8. Click **Apply**.

Encrypt Messages with OCF

You can use the Objectionable Content Filter (OCF) to create a dictionary of words that is checked against a message to indicate the message should be encrypted. For example, you may require that any outgoing messages that contain certain confidential information, for example, credit card information or medical records, must be encrypted. You can create an OCF dictionary listing the words to scan for in a message. If any of these words are found in the message, the message is encrypted before delivery.

1. Select **Security > Content Control > Objectionable Content**.
2. Select the **Enable OCF** check box.
3. In the **Outbound OCF** section, select the dictionary file that contains a list of words which indicate a message must be encrypted.
4. In the outbound **Email Action** drop-down list, select **SecureMail Encrypt**.
   Any outbound message containing words from the OCF dictionary file is encrypted before delivery.
5. Click **Apply**.

Encrypt Messages with Content Scanning

You can use a compliance dictionary to scan for specific words in the attachment of an outbound message that indicate a message must be encrypted. For example, your organization may require that any outgoing message attachments that contain certain confidential information, for example, credit card information or medical records, must be encrypted. You can create a compliance dictionary listing the words to scan for in the message attachment. If any of these words are found in the attachment, the message is encrypted before delivery.

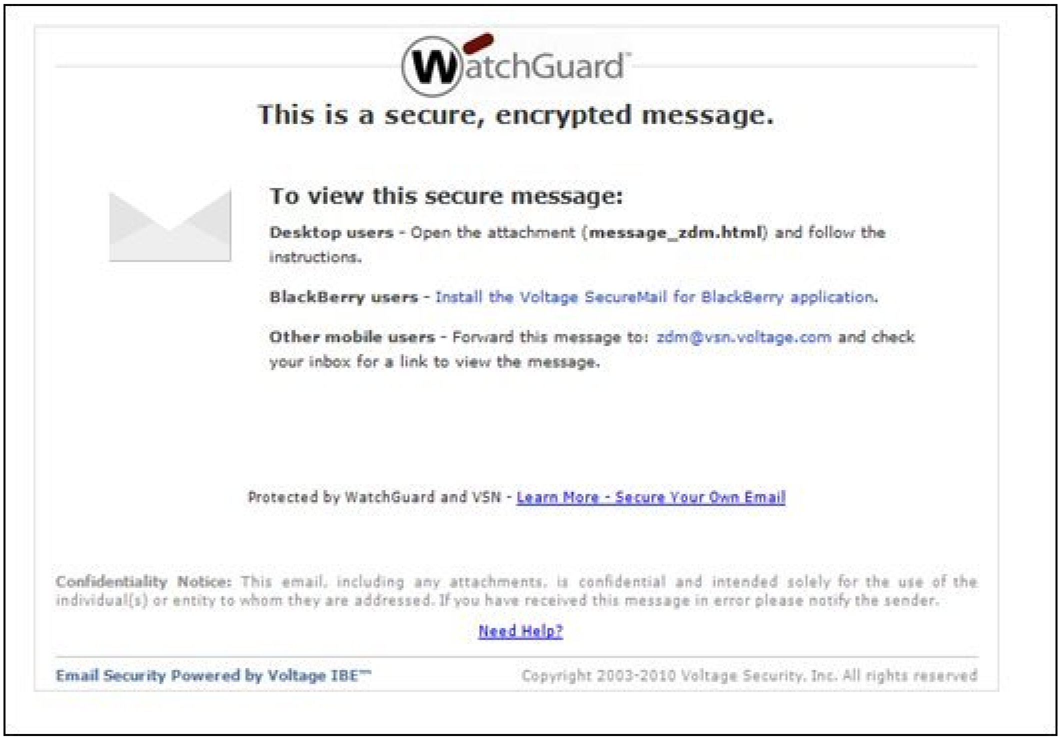
To configure Content Scanning to use encryption:

1. Make sure the Content Scanning feature is enabled globally in **Security > Content Control > Content Scanning**.
2. Select **Security > Policies > Policies**.
3. Select a specific policy.
4. Go to the **Content Scanning** section.
5. In the **Outbound Email Content Scanning** section, from the **Compliance Dictionaries** drop-down list, select the compliance file that contains a list of words which indicate a message must be encrypted.
6. In the **Action** field, click **Edit**, and select the **SecureMail Encrypt** action.
   Any outbound message with an attachment containing words from the compliance dictionary is encrypted before delivery.
7. Click **Apply**.

Read Encrypted Messages

To view an encrypted message:

1. When you receive an encrypted message, it appears similar to this message:



This is a secure, encrypted message.

To view this secure message:

Desktop users - Open the attachment (**message_zdm.html**) and follow the instructions.

BlackBerry users - Install the Voltage SecureMail for BlackBerry application.

Other mobile users - Forward this message to: zdm@vsn.voltage.com and check your inbox for a link to view the message.

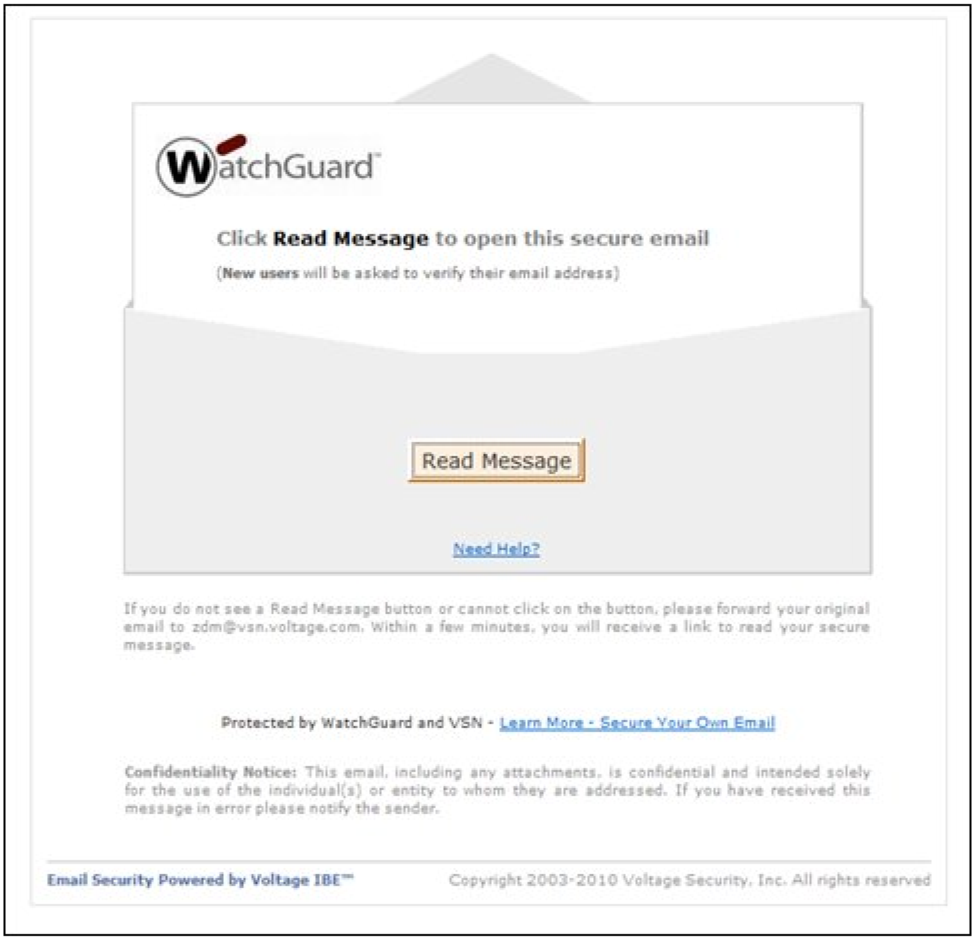
Protected by WatchGuard and VSN - Learn More - Secure Your Own Email

Confidentiality Notice: This email, including any attachments, is confidential and intended solely for the use of the individual(s) or entity to whom they are addressed. If you have received this message in error please notify the sender.

Need Help?

Email Security Powered by Voltage IBE™ Copyright 2003-2010 Voltage Security, Inc. All rights reserved

2. Open the message attachment "message_zdm.html".



Click **Read Message** to open this secure email

(**New users** will be asked to verify their email address)

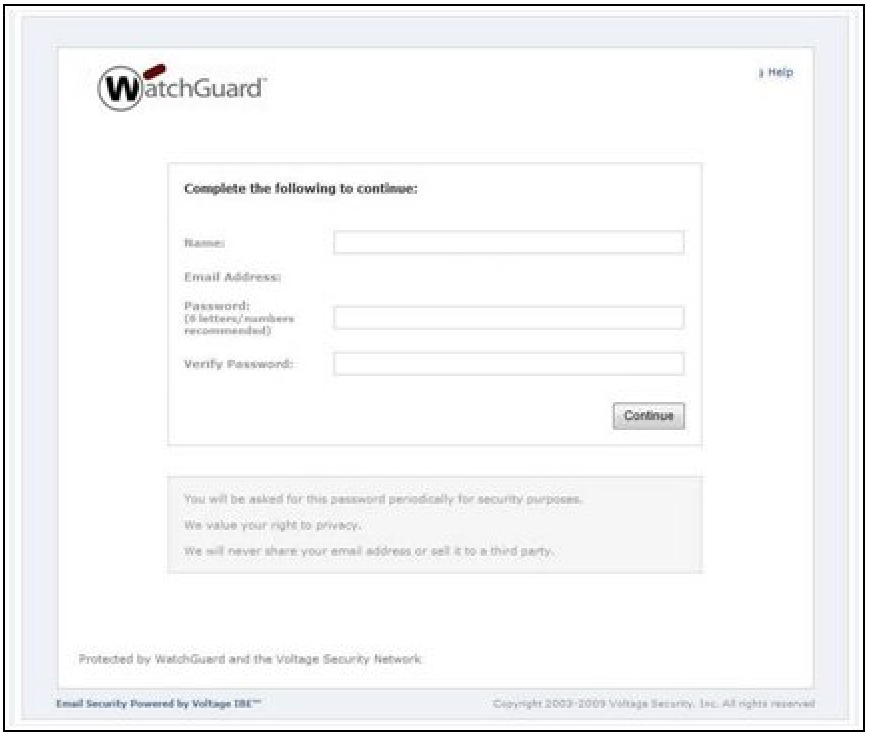
If you do not see a Read Message button or cannot click on the button, please forward your original email to zdm@vsn.voltage.com. Within a few minutes, you will receive a link to read your secure message.

Protected by WatchGuard and VSN - Learn More - Secure Your Own Email

Confidentiality Notice: This email, including any attachments, is confidential and intended solely for the use of the individual(s) or entity to whom they are addressed. If you have received this message in error please notify the sender.

Email Security Powered by Voltage IBE™ Copyright 2003-2010 Voltage Security, Inc. All rights reserved

3. Click **Read Message**.
4. If this is the first encrypted message you receive, you are prompted to register with the SecureMail service to create an account and establish a password.



Complete the following to continue:

Name:

Email Address:

Password:
(8 letters/numbers recommended)

Verify Password:

You will be asked for this password periodically for security purposes.

We value your right to privacy.

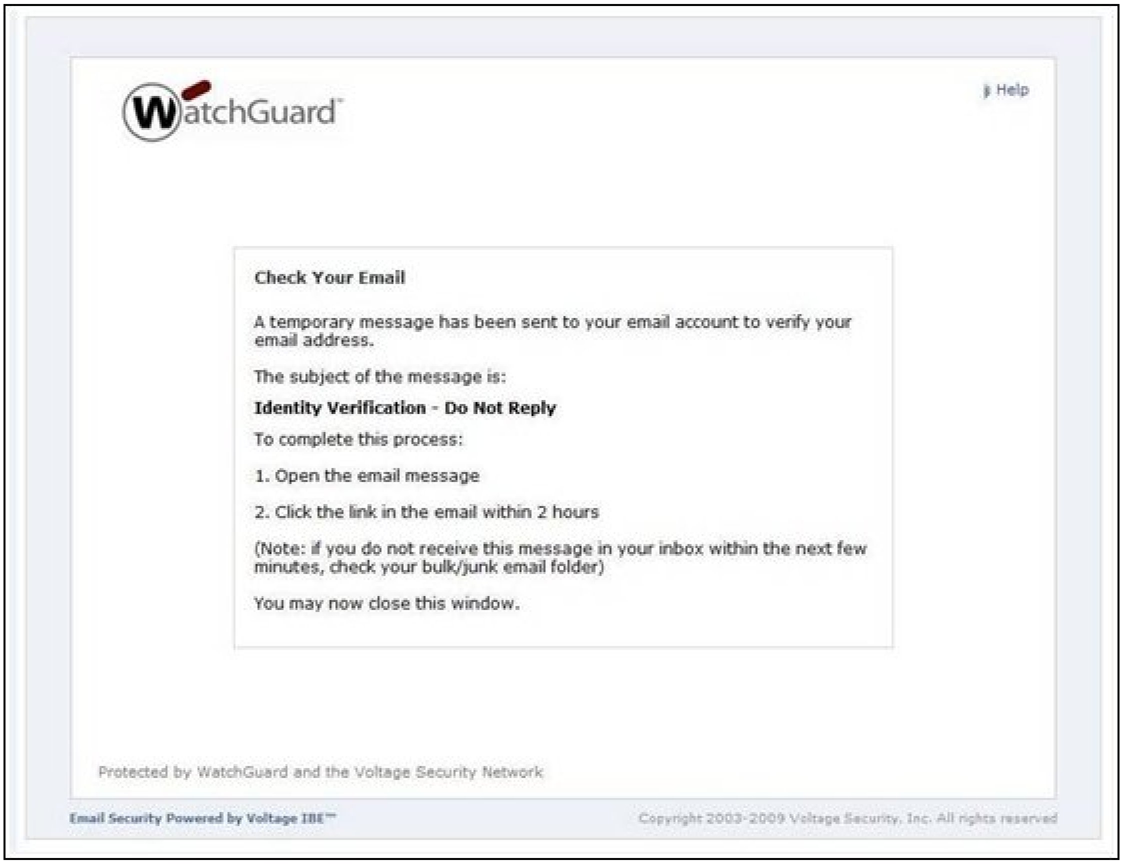
We will never share your email address or sell it to a third party.

Protected by WatchGuard and the Voltage Security Network

Email Security Powered by Voltage IBE™

Copyright 2003-2009 Voltage Security, Inc. All rights reserved

5. You must respond to a verification email message before you can open the encrypted message.



Check Your Email

A temporary message has been sent to your email account to verify your email address.

The subject of the message is:

Identity Verification - Do Not Reply

To complete this process:

1. Open the email message

2. Click the link in the email within 2 hours

(Note: if you do not receive this message in your inbox within the next few minutes, check your bulk/junk email folder)

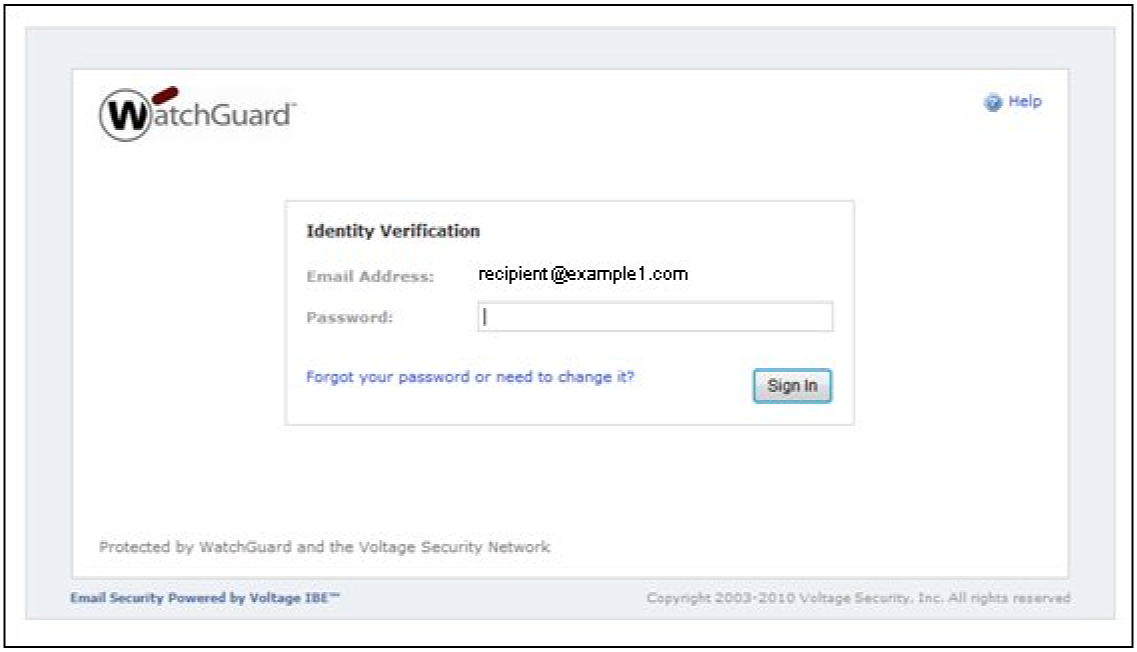
You may now close this window.

Protected by WatchGuard and the Voltage Security Network

Email Security Powered by Voltage IBE™

Copyright 2003-2009 Voltage Security, Inc. All rights reserved

6. You must type your password to verify your identity.



Identity Verification

Email Address: recipient@example1.com

Password:

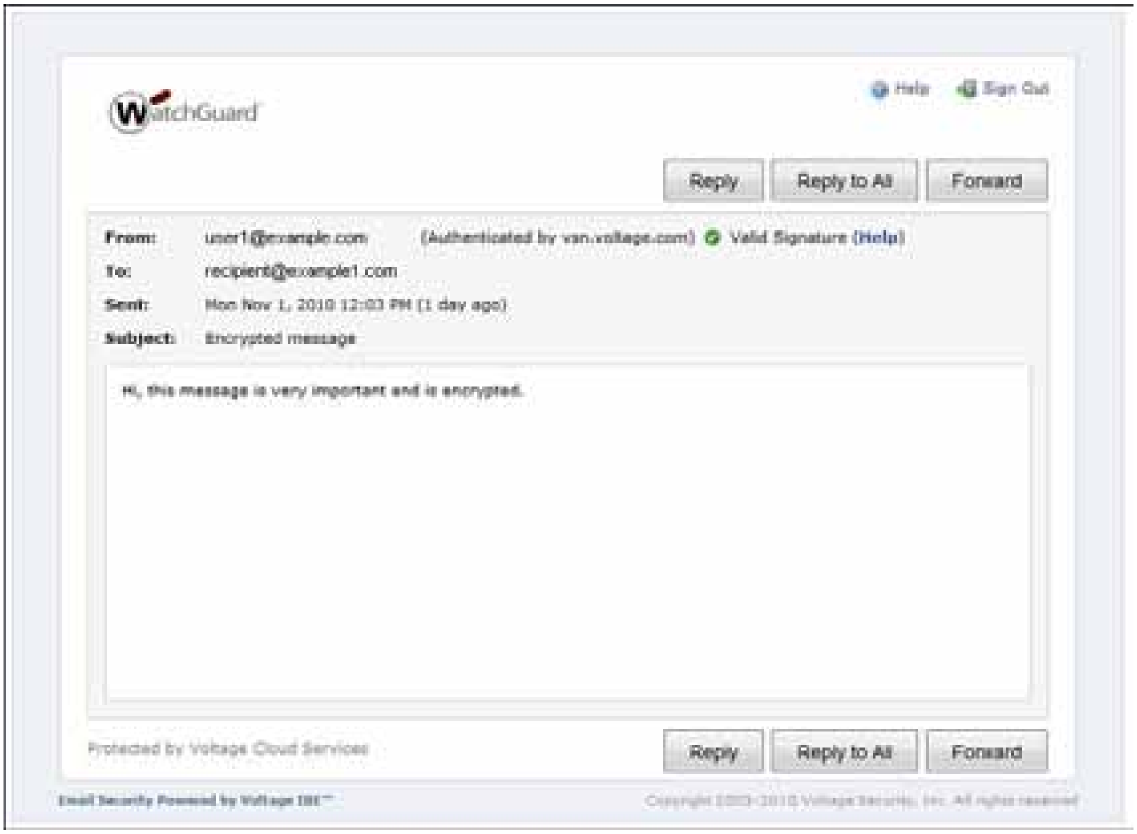
Forgot your password or need to change it?

Protected by WatchGuard and the Voltage Security Network

Email Security Powered by Voltage IBE™

Copyright 2003-2010 Voltage Security, Inc. All rights reserved

7. When you have authenticated to SecureMail, the secure message is decrypted and displayed.



From: user1@example.com (Authenticated by van.voltage.com) Valid Signature (Help)

To: recipient@example1.com

Sent: Mon Nov 1, 2010 12:03 PM (1 day ago)

Subject: Encrypted message

Hi, this message is very important and is encrypted.

Protected by Voltage Cloud Services

Email Security Powered by Voltage IBE™

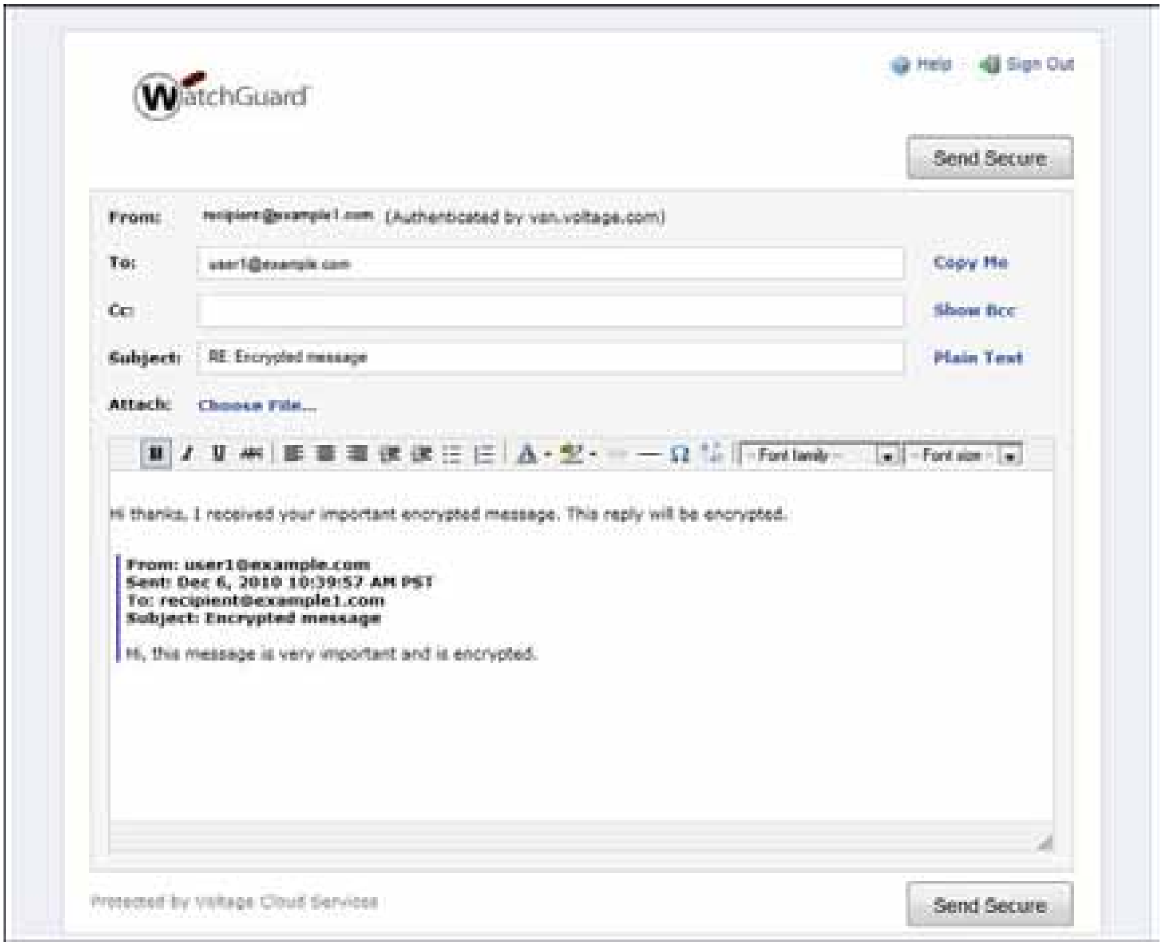
Copyright 2003-2010 Voltage Security, Inc. All rights reserved

Reply to Encrypted Messages

You can securely reply to or forward encrypted messages within the same web-based service that allows you to read the encrypted message.

To reply to an encrypted email message on the SecureMail web site:

1. From the encrypted message, click **Reply**, **Reply All**, or **Forward**.



From: recipient@example1.com (Authenticated by van.voltage.com)
To: user1@example.com
Cc:
Subject: RE: Encrypted message
Attach: Choose File...

Hi thanks, I received your important encrypted message. This reply will be encrypted.

> **From: user1@example.com**
> **Sent: Dec 6, 2010 10:39:57 AM PST**
> **To: recipient@example1.com**
> **Subject: Encrypted message**
>
> Hi, this message is very important and is encrypted.

Protected by Voltage Cloud Services

2. Type your reply.
3. Click **Send Secure**.
   An encrypted reply is sent to the sender of the original encrypted message.

The SecureMail server sends secure replies on behalf of your organization's email domain, and the email message will appear as originating from a SecureMail domain. In certain cases, your mail security devices may block these messages because they originate from a different domain than your own. You must make sure that your mail security devices are configured to allow messages from SecureMail servers when secure replies are sent back to your email domain.

On the WatchGuard XCS, you can configure *Pattern Filters* to "Accept" these SecureMail IP addresses:

Host	IP Address	Notes
mail1.vsn.voltage.com	165.193.228.181, 205.140.196.245*	*This IP will eventually replace the existing mail1 host address
mail2.vsn.voltage.com	165.193.228.186, 205.140.196.250*	*This IP will eventually replace the existing mail2 host address
mail3.vsn.voltage.com	165.193.91.245	
mail4.vsn.voltage.com	165.193.91.250	

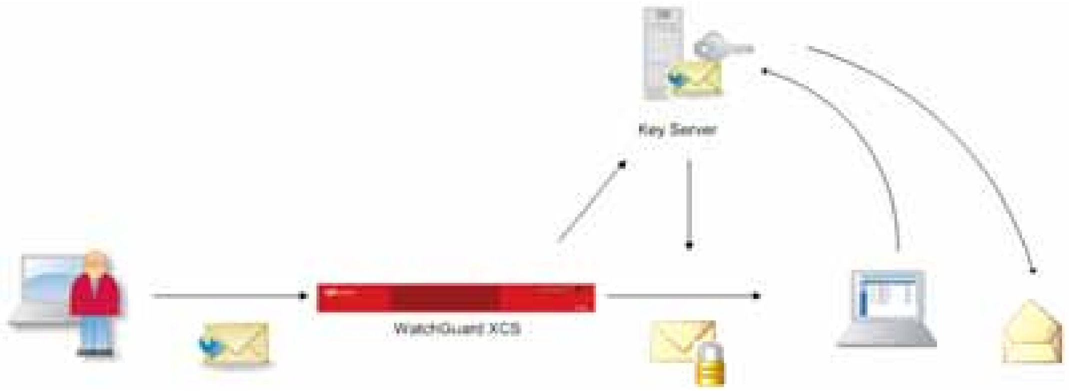
PostX Mail Encryption

Integrated message encryption allows users to encrypt outbound messages directly from the WatchGuard XCS without the need for a local encryption server or additional desktop software. Messages are secured until they are delivered and decrypted by the recipient of the message.

The Encryption Option allows organizations to easily enforce company policies and compliance regulations with the secure delivery of encrypted messages without the need for the recipient to download or install any special software. The Encryption Option uses the PostX Cisco Registered Envelope Service which creates an encrypted message for the recipient that can be read by opening an attachment to provide access to the decrypted message.

You can use a public key server for services and key-exchange related activities, or to use a local key server in your organization.

How Message Encryption Works



1. When a user sends a message, the system uses pattern and content filters to determine if a specific encryption policy applies to the message.
2. If the policy applies, the system uses its integrated encryption engine to encrypt the message by communicating with the key server (either a public server or a local key server) to retrieve the session key for the message.
3. The message is encrypted and delivered to the recipient as an attachment.

4. The recipient opens the attachment to allow them to register (if this is the first encrypted message received) and authenticate to the Cisco Registered Envelope Service web site.
5. The Registered Envelope Service web site uses the session key to allow the user to read the unencrypted message.

Cisco Registered Envelope Service (CRES)

The Registered Envelope Service is a push service that sends secure, encrypted messages directly to a recipient's inbox. The WatchGuard XCS integrates this feature to allow message to be encrypted on the system before it is delivered to the intended recipient. The recipient does not require any additional software or configuration to decrypt and read the message. You can open Registered Envelopes from any email platform, on any operating system and web browser.

The Registered Envelope Service architecture allows the system's integrated encryption software to perform the message encryption and message delivery functions directly on your appliance, while the hosted system provides services, for example, key management, user accounts, online opening, and secure reply to messages.

Messages from your organization are never viewed, hosted or stored by the Registered Envelope Service in any form.

These features are available when using the CRES service:

- **User Enrollment** – When a recipient receives a secure message for the first time, they are prompted to register to create an account and establish a password. The password is used to open this message and all future encrypted messages from the same organization.
- **Logging** – Each Registered Envelope message is logged, and you can view its status. You can track the message to obtain proof that the message has been opened and read by the recipient.
- **Message Locking** – Encrypted messages are locked if they have not been read by the recipient before the specified expiration time. You can also manually block messages to prevent specific messages from being opened and decrypted.
- **Message Expiration** – Encrypted messages can be set to expire after a certain date. After the message expires, it is locked and it cannot be opened by the intended recipient. This makes sure that time-sensitive secure messages expire if they are not read in the designated expiration time.
- **SecureReply** – Recipients can immediately reply to encrypted messages they receive using a secure mechanism to preserve the integrity of the original email. The recipients can compose the reply within the web-based service that encrypts the message before it is sent back to the original sender.

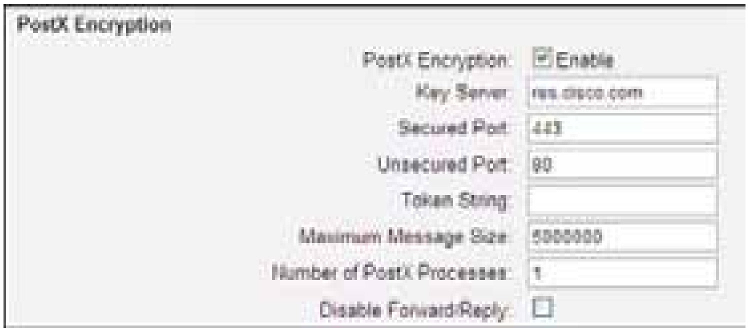
Encryption Configuration on the WatchGuard XCS

When message encryption is enabled globally, you can identify outgoing messages for encryption using Pattern Filters, Objectionable Content Filtering, and Content Scanning through policies.

> ***Note*** *Messages to local mailboxes on the system are not encrypted. Internal mail boxes are already secured and do not require further protection by encryption.*

To configure integrated message encryption:

1. Select **Security > Encryption > PostX**.



PostX Encryption

PostX Encryption:	☑ Enable
Key Server:	res.cisco.com
Secured Port:	443
Unsecured Port:	80
Token String:	
Maximum Message Size:	5000000
Number of PostX Processes:	1
Disable Forward/Reply:	□

2. Select the **PostX Encryption** check box to enable encryption globally for outgoing messages.

   If you disable encryption globally, all outgoing messages from the system are sent in clear text. When you enable encryption, you must create Pattern Filters or use OCF/Content Scanning to identify messages for encryption. You must also upload a token file or define a token string for use with a public key server. If you disable encryption globally, existing encryption filters still trigger and the message is queued and deferred to prevent the message from being delivered in unencrypted clear text. These filters must be disabled or deleted if you disable the Encryption option.

3. In the **Key Server** text box, type the server address to use to encrypt and decrypt messages.

   The default is res.cisco.com. You must have an account with the Cisco Registered Envelope Service and a valid token file or token string. You can also specify the address of a local key server if you are not using the public key server.

4. In the **Secure Port** text box, type the port to use for secure communications by the public key server or a local key server.

   By default, the public key server listens on port 443. A local key server listens on port 8443.

5. In the **Unsecure Port** text box, type the port to use for unsecured communications by the public key server or a local key server.

   By default, the public key server listens on port 80. A local key server listens on port 8080.

6. In the **Token String** text box, type the string provided with your license to identify your account when communicating with the key server.

   In some cases, only a token file is required and the token string field remains undefined. If both are configured, the token string takes precedence.

7. In the **Maximum Message Size** text box, type the maximum size of message (in bytes) that is accepted for encryption.

   Mail larger than this size that is marked for encryption is rejected. This prevents very large messages from causing latency with the encryption engine. You can enter values between 0 and 1,000,000,000. The default is 5,000,000 bytes. Type `0` to specify no limit.

8. In the **Number of PostX Processes** text box, specify the maximum processes available to encrypt messages.

   Each encryption process can simultaneously encrypt one message. The default is 1. Encryption is a CPU-intensive process and you should use caution when you increase this value.

9. To remove the “Forward”, “Reply”, and “Reply to All” buttons when a user views an encrypted message, select the **Disable Forward/Reply** check box.
10. You can customize the **Message Header** and **HTML Message Header** that provides the recipient with instructions on how to read the encrypted message.

    If this is the first time the recipient receives an encrypted message, they are prompted to register with the Registered Envelope Service to create an account login and password. The password is used to open this message and any future encrypted messages from the specified organization.

Get a Token File

After you establish a CRES account, you must upload a token file to the WatchGuard XCS. This token file is used to identify your account when communicating with the key server. You can download the token file from your Cisco Registered Envelope Service web account.

To download your token file:

1. Log in to your Cisco Registered Envelope Service management account.
2. Select **Accounts > Manage Accounts**, and select your account number.
3. Select **Tokens**.
4. Click the “Save Token” icon in the **Actions** column to download the Default Token file to your local computer.
   Do not download the “SecureCompose” token to the WatchGuard XCS.

Upload a Token File to the WatchGuard XCS

1. On the WatchGuard XCS, select **Security > Encryption > PostX**.
2. Click **Upload Token**.
3. Type the name of the token file, or click **Browse** to find the file on your local computer.
4. Click **Upload**.
   If you use a local key server and not the public key servers, the token file is retrieved directly from the local server.

> ***Note*** *Token files are not replicated to other members of a Cluster and you must apply the token file manually to each cluster system.*

Encrypt Messages with Pattern Filters

You can create Pattern Filters to search for text in an outgoing message that identifies it as a message to be encrypted. For example, you can create a filter to search for the text “Encrypt” in a subject header to indicate the message must be encrypted before it is sent to its destination.

To configure a Pattern Filter:

1. Select **Security > Content Control > Pattern Filters**.
2. Click **Add**.
3. Create an outbound filter that searches for the words “Encrypt” in the subject of a message.
4. From the **Action** drop-down list, select **PostX Encrypt**.
   Any outbound message with the word “Encrypt” in the subject is encrypted before delivery.

Encrypt Messages with OCF

You can use the Objectionable Content Filter (OCF) to create a dictionary of words that is checked against a message to indicate the message should be encrypted. For example, you may require that any outgoing messages that contain certain confidential information, for example, credit card information or medical records, must be encrypted. You can create an OCF dictionary listing the words to scan for in a message. If any of these words are found in the message, the message is encrypted before delivery.

1. Select **Security > Content Control > Objectionable Content**.
2. Select the **Enable OCF** check box.
3. In the **Outbound OCF** section, select the dictionary file that contains a list of words which indicate a message must be encrypted.
4. In the outbound **Email Action** drop-down list, select **PostX Encrypt**.
   Any outbound message containing words from the OCF dictionary file is encrypted before delivery.
5. Click **Apply**.

Encrypt Messages with Content Scanning

You can use a compliance dictionary to scan for specific words in the attachment of an outbound message that indicate a message must be encrypted. For example, your organization may require that any outgoing message attachments that contain certain confidential information, for example, credit card information or medical records, must be encrypted. You can create a compliance dictionary listing the words to scan for in the message attachment. If any of these words are found in the attachment, the message is encrypted before delivery.

To configure Content Scanning to use encryption:

1. Make sure the Content Scanning feature is enabled globally in **Security > Content Control > Content Scanning**.
2. Select **Security > Policies > Policies**.
3. Select a specific policy.
4. Go to the **Content Scanning** section.
5. In the **Outbound Email Content Scanning** section, from the **Compliance Dictionaries** drop-down list, select the compliance file that contains a list of words which indicate a message must be encrypted.
6. In the **Action** field, click **Edit**, and select the **PostX Encrypt** action.
   Any outbound message with an attachment containing words from the compliance dictionary is encrypted before delivery.
7. Click **Apply**.

CRES Account Administration

The Cisco Registered Envelope Service provides a web-based management console to allow you to perform these tasks:

- Manage Accounts and Token Files
- Manage Images (message branding)
- Manage Users
- Generate message activity reports
- Manage secure messages and perform delivery and response tracking

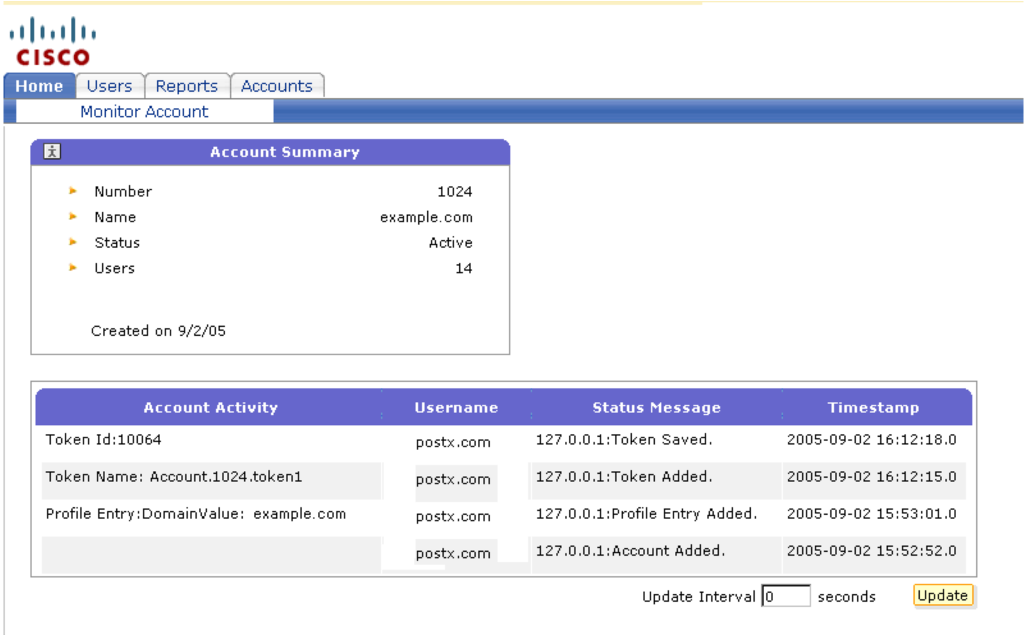
Access the management console at this URL:

```
https://res.cisco.com/admin/
```

Manage Accounts

You can manage your CRES account with the web-based administration console. This allows you to manage users, manage encrypted messages, perform delivery and response tracking, and generate message activity reports.

From the main home page, account information for your organization is displayed. This includes the organization's current status, the number of users registered, and token file information.



Account Summary

Number	1024
Name	example.com
Status	Active
Users	14

Created on 9/2/05

Account Activity	Username	Status Message	Timestamp
Token Id:10064	postx.com	127.0.0.1:Token Saved.	2005-09-02 16:12:18.0
Token Name: Account.1024.token1	postx.com	127.0.0.1:Token Added.	2005-09-02 16:12:15.0
Profile Entry:DomainValue: example.com	postx.com	127.0.0.1:Profile Entry Added.	2005-09-02 15:53:01.0
	postx.com	127.0.0.1:Account Added.	2005-09-02 15:52:52.0

Update Interval 0 seconds Update

Manage Token Files

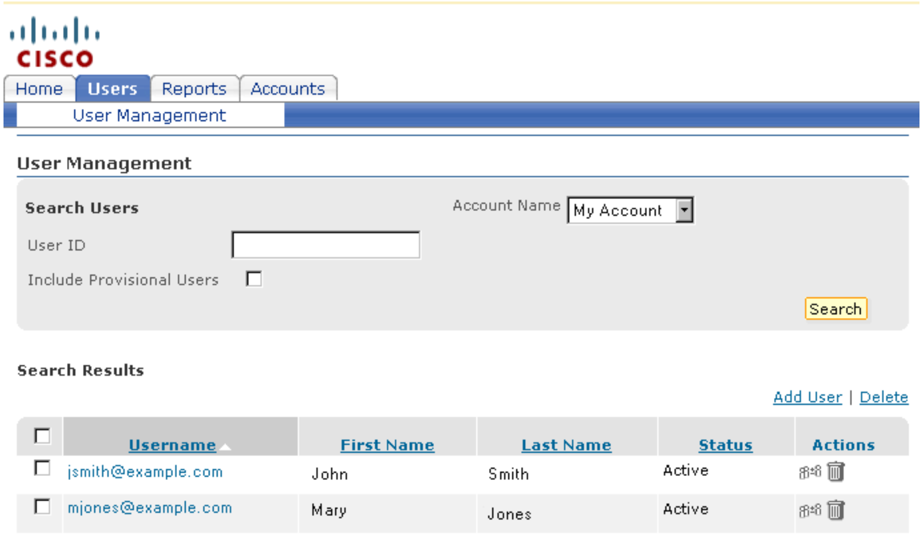
The token file identifies your organization's account when communicating with the key server. You must retrieve your token file from the CRES management account and upload it to the WatchGuard XCS. See *Upload a Token File to the WatchGuard XCS* for more detailed information on uploading a token file.

Manage Images

You can customize the logo that appears on Registered Envelope messages to reflect your own corporate branding.

Manage Users

Select the **Users** tab to administer your users. Individual user accounts are not required for users in your organization to send out secure encrypted messages, but you must enroll users to be able to decrypt and read encrypted messages or track sent messages. You can also add additional administrative users from this menu.



User Management

Search Users

Account Name: My Account

User ID

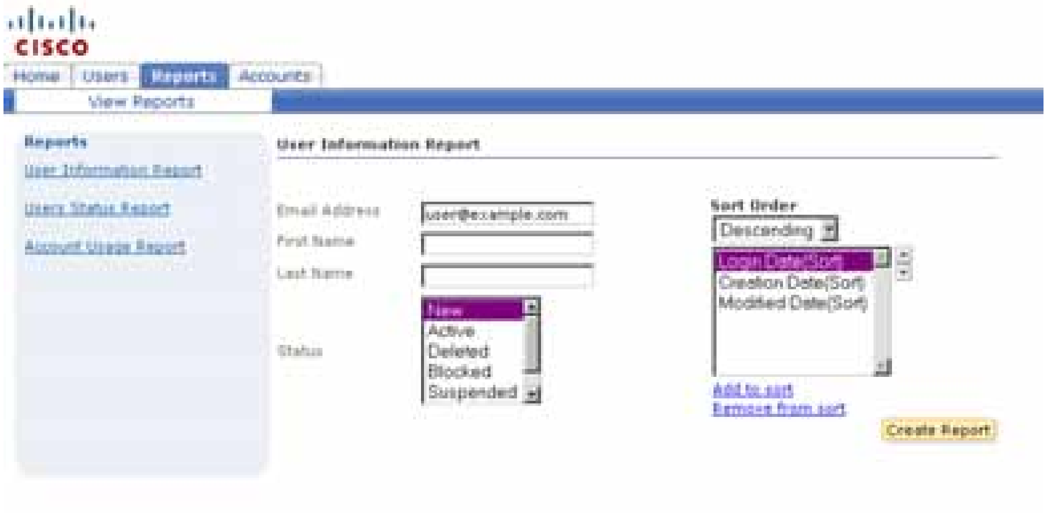
Include Provisional Users □

Search Results

□	Username	First Name	Last Name	Status	Actions
□	jsmith@example.com	John	Smith	Active	
□	mjones@example.com	Mary	Jones	Active	

Generate Message Activity Reports

In the **Reports** menu, you can create account usage reports, and filter the results with the From or To fields, the timestamp, and status of the message.



User Information Report

Email Address: user@example.com

First Name

Last Name

Status: New, Active, Deleted, Blocked, Suspended

Sort Order: Descending

Login Date(Sort)
Creation Date(Sort)
Modified Date(Sort)

Manage Secure Messages

In the **Accounts > Manage Registered Envelopes** menu, you can view the status of encrypted messages sent by your organization. Each message entry displays these fields:

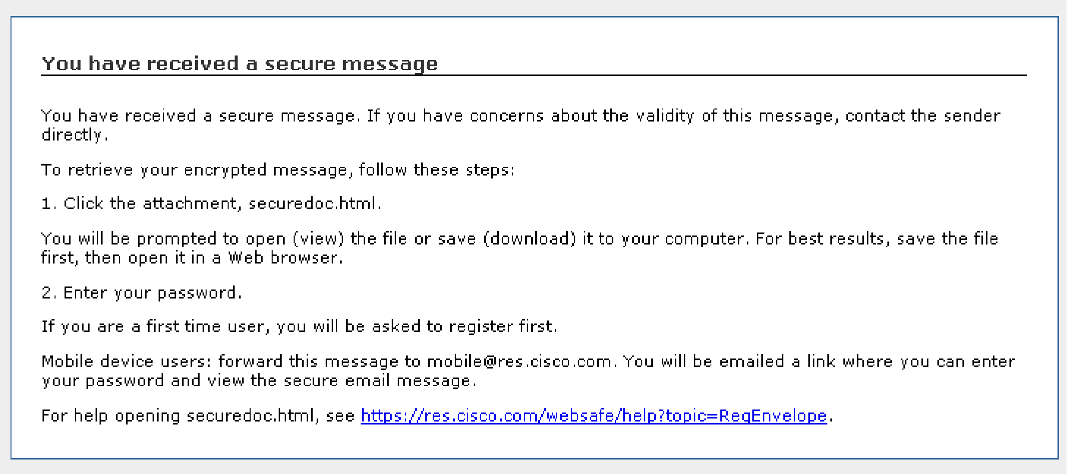
- **From** – Displays who sent the message.
- **To** – Displays the message recipients.
- **Subject** – The subject of the message.
- **Sent** – The time and date the message was sent.
- **Opened** – Indicates when the message was opened by the recipient. The field is blank if the message is unread.

- **Expires**– Indicates when the secure message expires. If the recipient does not open the message before the expiration date, the message is locked and further attempts to open the message fail. To modify expiration dates, select a message or group of messages and then click **Update Expiration Dates**.
- **Locked** – Indicates if the message is locked because it is expired or if the you have manually locked the message to prevent viewing. To manually lock or unlock messages, select a message or group of messages, and then click **Lock/Unlock Envelopes**.
- **Reason** – Displays information or an error status about the message. You can enter text in the **Reason** field if you manually lock a message.

You can search for messages by date and by keywords in the **From**, **To**, **Subject**, and **Reason** fields.

Read Encrypted Messages

When the recipient receives an encrypted message, it appears in their inbox and appears similar to this message:



You have received a secure message

You have received a secure message. If you have concerns about the validity of this message, contact the sender directly.

To retrieve your encrypted message, follow these steps:

1. Click the attachment, securedoc.html.

You will be prompted to open (view) the file or save (download) it to your computer. For best results, save the file first, then open it in a Web browser.

2. Enter your password.

If you are a first time user, you will be asked to register first.

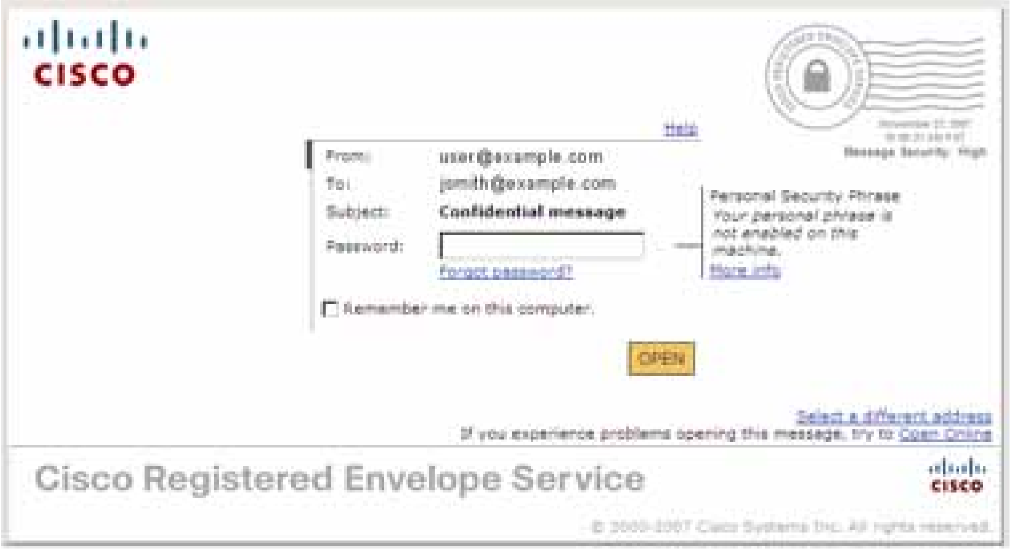
Mobile device users: forward this message to mobile@res.cisco.com. You will be emailed a link where you can enter your password and view the secure email message.

For help opening securedoc.html, see https://res.cisco.com/websafe/help?topic=RegEnvelope.

The recipient is prompted to open a message attachment called “securedoc.html”.

If this is the first encrypted message received by the recipient, when they open the attachment, they are prompted to register with the Cisco Registered Envelope Service to create an account and establish a password.

The new account and password are used to open this message and all other encrypted messages sent from the same organization. The recipient is prompted to enter the password to log in and read the message:



From: user@example.com
To: jsmith@example.com
Subject: **Confidential message**
Password:
Forgot password?

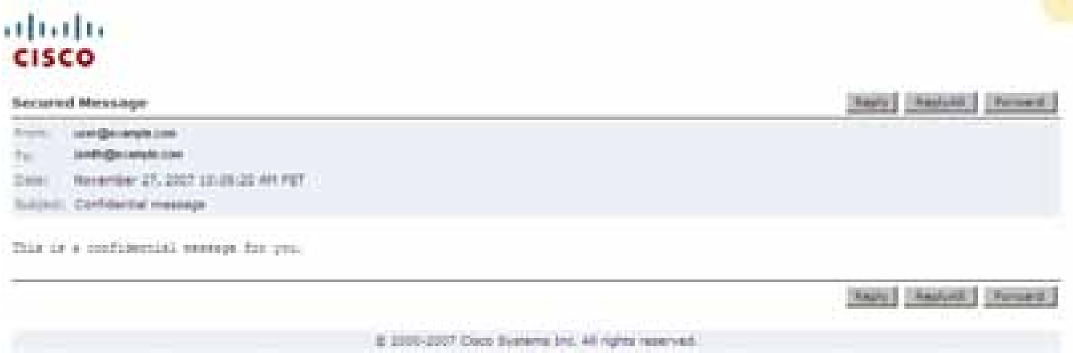
Personal Security Phrase
Your personal phrase is not enabled on this machine.
More info

□ Remember me on this computer.

Select a different address
If you experience problems opening this message, try to Open Online

© 2000-2007 Cisco Systems Inc. All rights reserved.

When the user is authenticated, the secure message is decrypted and displayed:



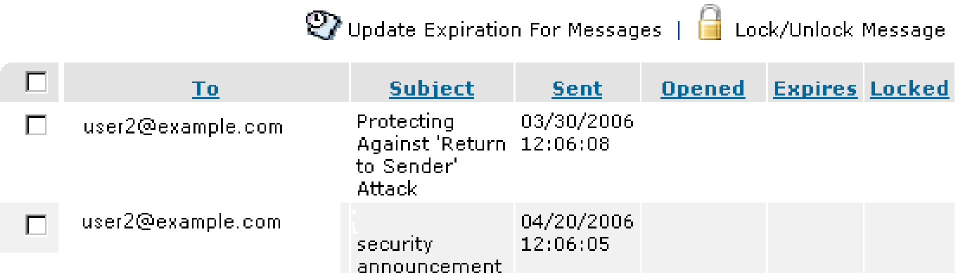
From: user@example.com
To: jsmith@example.com
Date: November 27, 2007 12:05:22 AM PST
Subject: Confidential message

This is a confidential message for you.

© 2000-2007 Cisco Systems Inc. All rights reserved.

Track Encrypted Messages

Users who have sent an encrypted message can track the status of the message using their CRES account. After the user logs in, their profile appears and displays any secure messages recently sent.



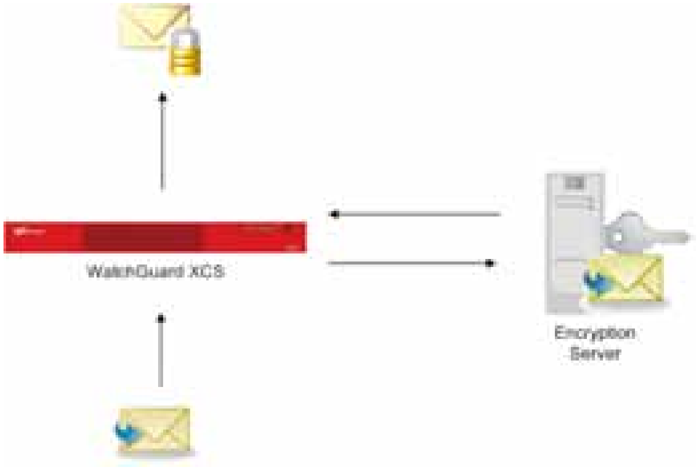
□	To	Subject	Sent	Opened	Expires	Locked
□	user2@example.com	Protecting Against 'Return to Sender' Attack	03/30/2006 12:06:08			
□	user2@example.com	security announcement	04/20/2006 12:06:05			

- **To** – Displays the message recipients.
- **Subject** – The subject of the message.
- **Sent** – The time and date the message was sent.

- **Opened** – Indicates when the message was opened by the recipient. The field is blank if the message is unread.
- **Expires** – Indicates when the secure message expires. If the recipient does not open the message before the expiration date, the message is locked and further attempts to open the message fail. To modify expiration dates, select a message or group of messages, and then click **Update Expiration for Messages**.
- **Locked** – Indicates if the message is locked due to being expired or if the message has been manually locked by the sender or the administrator. To manually lock or unlock a message, select a message or group of messages, and then click **Lock/Unlock Message**.

External Email Message Encryption

The WatchGuard XCS provides integration with external encryption servers to provide email encryption and decryption functionality. Email encryption allows individual messages to be encrypted by a separate encryption server before they are delivered to their destinations. An incoming encrypted message can also be sent to the encryption server to be decrypted before the system accepts the message and delivers it to the intended recipient. This integration allows organizations to make sure that encrypted messages are still processed to detect security, content, and policy issues.



Email encryption provides organizations with the ability to protect the privacy and confidentiality of their messages and also to conform with any regulatory compliance policies that must make sure that certain types of data are encrypted before they are sent out across the Internet. Encryption and decryption is performed for selected email messages with filter rules on the WatchGuard XCS. A message filter is created for specific email sending addresses, IP addresses and host names of specific SMTP servers, or for specific words located in the subject of a message, for example, “Encrypt”.

Because mail is forwarded back and forth between the WatchGuard XCS and the Encryption server, all mail statistics include this additional delivery information.

To configure external message encryption and decryption:

1. Configure the encryption server to integrate with the WatchGuard XCS.
2. Create mail routes to the encryption server on the WatchGuard XCS.
3. Enable encryption and decryption on the WatchGuard XCS.
4. Create encryption rules on the WatchGuard XCS to identify messages to encrypt.

> ***Note*** *The Encryption server must be on the same network as the WatchGuard XCS. Use the ping utility to make sure they are communicating properly and can see each other on the network.*

Configure the Encryption Server

The existing encryption server must be set up to relay all mail to the WatchGuard XCS. Please see the documentation provided by your encryption server vendor. Typically, outbound and inbound proxies or mail routes must be configured on the encryption server to make sure messages are accepted from and passed back to theWatchGuard XCS after they are encrypted or decrypted.

Define Mail Routes for Encryption and Decryption

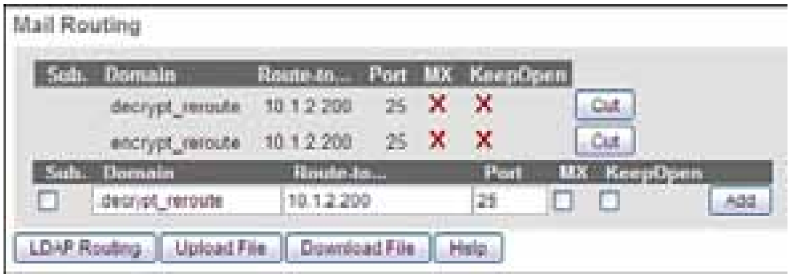
You must define Mail routes to the encryption server for both encrypting and decrypting messages. To make sure the system knows where to route messages for encryption, create a mail route for the domains `.encrypt_reroute` and `.decrypt_reroute` to the address of the encryption server.

Select **Configuration > Mail > Routing**.

1. In the **Domain** text box, type`.encrypt_reroute`
2. In the **Route-to** text box, type the address of the encryption server.

   For example, `10.1.2.200`
3. Click **Add**.
4. In the **Domain** text box, type`.decrypt_reroute`
5. In the **Route-to** text box, type the address of the encryption server.

   For example, `10.1.2.200`
6. Click **Add**.



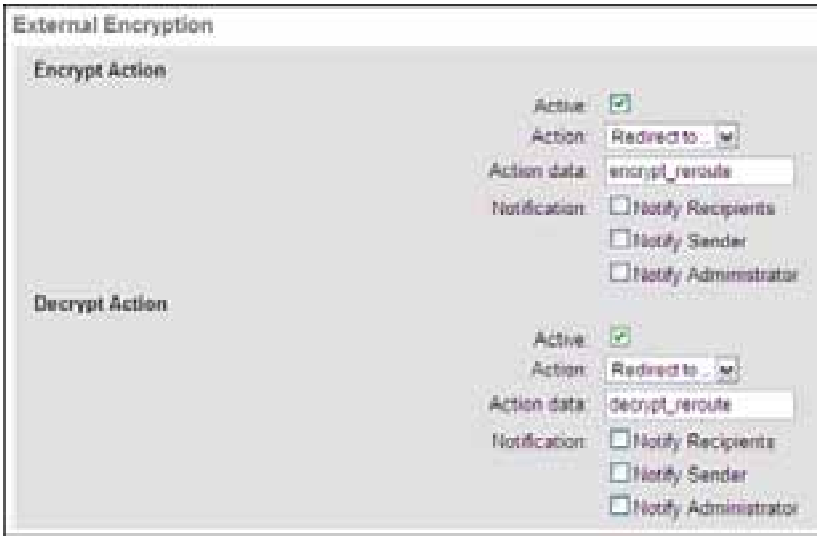
Mail Routing

Sub.	Domain	Route-to...	Port	MX	KeepOpen	
	decrypt_reroute	10.1.2.200	25	✗	✗	Cut
	encrypt_reroute	10.1.2.200	25	✗	✗	Cut

Sub.	Domain	Route-to...	Port	MX	KeepOpen	
□	decrypt_reroute	10.1.2.200	25	□	□	Add

Enable Encryption and Decryption on the WatchGuard XCS

1. Select **Security > Encryption > External**.
   The External Encryption page appears.



External Encryption

Encrypt Action

Active: ☑

Action: Redirect to ...

Action data: encrypt_reroute

Notification: □ Notify Recipients

□ Notify Sender

□ Notify Administrator

Decrypt Action

Active: ☑

Action: Redirect to ...

Action data: decrypt_reroute

Notification: □ Notify Recipients

□ Notify Sender

□ Notify Administrator

2. Select the **Active** check box for the **Encrypt Action** and **Decrypt Action** section.
3. From the **Action** drop-down list, select **Redirect to**.
4. In the **Action data** text box, type `encrypt_reroute` or `decrypt_reroute` for the required section.
5. Select who to send notifications to when a message is encrypted or decrypted. You can select **Notify Recipient**, **Notify Sender**, or **Notify Administrator**.
6. Click **Apply**.

Define Filter Rules for Encryption

You must use a filer rule to identify what types of messages to encrypt. For example, your organization may use a tag in the subject header, for example, “Encrypt”, which is used to identify an outgoing message that must be encrypted. You can also define specific email addresses and IP addresses to make sure certain users or servers have their email encrypted.

You can create encryption rules with Pattern Filters or by using definable dictionaries with the Objectionable Content and Content Scanning features. The latter features allow you to use dictionaries with specific keywords and phrases to trigger the encryption rules.

The filter rule examines outbound mail messages for specific patterns to redirect mail for encryption. This pattern can be a user’s email address or a phrase in the subject header.

To set up an encryption rule with Pattern Filters:

1. Select **Security > Content Control > Pattern Filters**.
2. Click **Add**.
3. Create a simple rule that checks all outbound mail for the word “Encrypt” in the subject, and set the action to **Encrypt**.
4. Create a rule to match the **Client IP** field to the address of the Encryption server, for example `10.1.2.200`, and set the action to **Relay**.

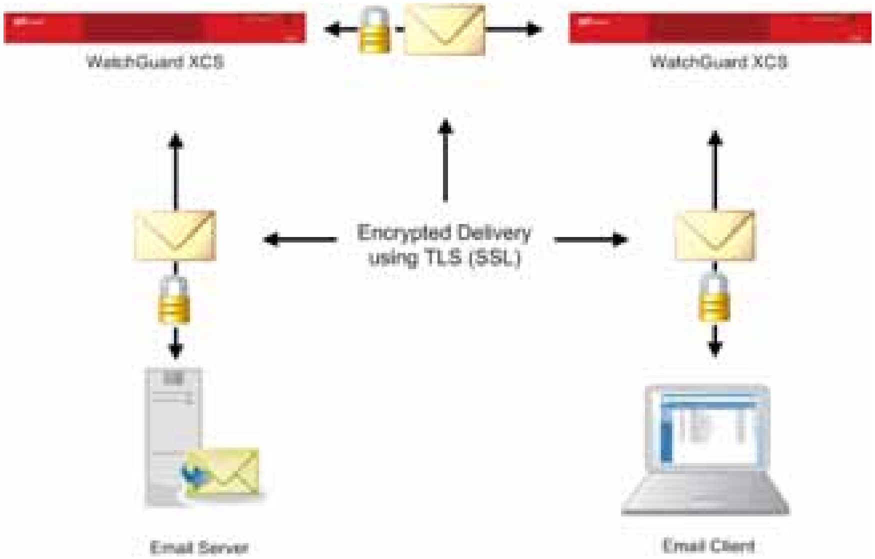
   You must create a separate filter rule to relay messages arriving from the encryption server. This action allows the system to accept messages back from the encryption server that have been encrypted and relay these messages to external networks. The filter rule that relays messages back must be of a higher priority than any encryption rule.

You must create a similar Pattern Filter rule to examine incoming messages that need to be decrypted before they are delivered to the recipient.

5. Click **Apply**.

Encrypt Mail Delivery Sessions

The WatchGuard XCS offers a simple mechanism to encrypt mail delivery with SSL (Secure Socket Layer) and TLS (Transport Layer Security) encryption. You can implement a flexible policy to allow other servers and clients to establish encrypted sessions with the WatchGuard XCS to send and receive mail.



You can encrypt these types of traffic:

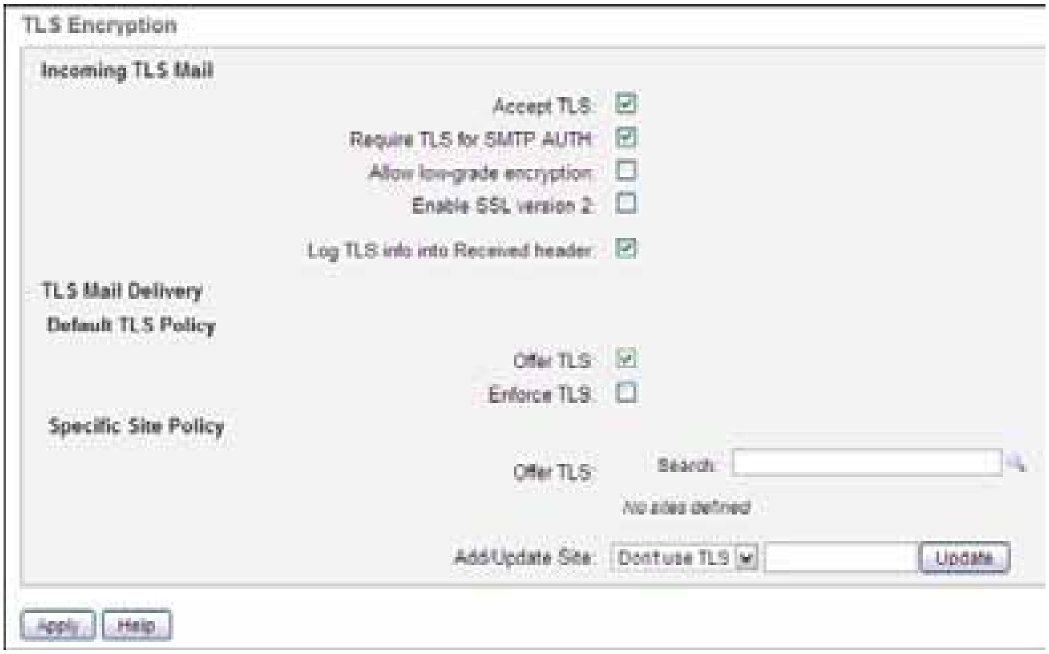
- **Server to Server** – Creates an email VPN (Virtual Private Network) and protects company email over the Internet.
- **Client to Server** – Use email clients, for example, Outlook with TLS, to send and receive mail. This allows email messages to be sent with complete confidentiality from desktop to desktop, but without the difficulties of implementing other encryption schemes.

You can enforce encryption between servers, for example, you can set up an email VPN between two WatchGuard XCS systems at remote sites. Encryption can also be optional so that users who are concerned about the confidentiality of their messages on the internal network can specify encryption in their mail client when it communicates with the WatchGuard XCS. The WatchGuard XCS supports the use of certificates to initiate the negotiation of encryption keys. The system can generate its own site certificates, and can also import Certificate Authority (CA) signed certificates.

See *Certificates* for more information on importing certificates.

To configure mail delivery encryption:

1. Select **Security > Encryption > TLS**.
   The TLS Encryption page appears.



TLS Encryption

Incoming TLS Mail

Accept TLS: ☑

Require TLS for SMTP AUTH: ☑

Allow low-grade encryption: □

Enable SSL version 2: □

Log TLS info into Received header: ☑

TLS Mail Delivery

Default TLS Policy

Offer TLS: ☑

Enforce TLS: □

Specific Site Policy

Offer TLS: Search:

No sites defined

Add/Update Site: Dont use TLS

2. Select the **Accept TLS** check box to accept SSL/TLS for incoming mail connections.
3. To require SSL/TLS when accepting mail for authenticated relay, select **Require TLS for SMTP AUTH**.
4. To allow the use of low-grade encryption ciphers for incoming TLS connections, for example, 64-bit DES, select the **Allow low-grade encryption** check box.
   This option may need to be enabled to support older mail servers, but reduces connection security.
5. Clear the **Enable SSL version 2** check box to disable older SSL versions for security audit testing.
   Disabling SSL version 2 may prevent older mail systems from sending mail with TLS.
6. To log TLS information (this includes protocol, cipher used, client and issuer common name) into the Received: message header, select the **Log TLS info into Received header** check box.
   These headers can be modified by intermediate servers and only information recorded at the final destination is reliable.
7. To offer remote mail servers the option of using SSL/TLS when sending mail, select the **Offer TLS** check box.
8. To require the validation of a CA-signed certificate when delivering mail to a remote mail server, select the **Enforce TLS** check box.

   If the certificate validation fails, the mail delivery connection is denied.
9. Click **Apply**.

Specific Site Policy

The **Specific Site Policy** option supports the specification of exceptions to the default settings for TLS/SSL. For example, you may need to exempt a mail server from using TLS/SSL because of lack of TLS support.

> ***Note*** *When you enable TLS, create policies to improve performance for internal hosts that do not need to send or receive with TLS.*

To exempt a server from TLS:

1. From the **Add/Update Site** drop-down list, select **Don't Use TLS**.

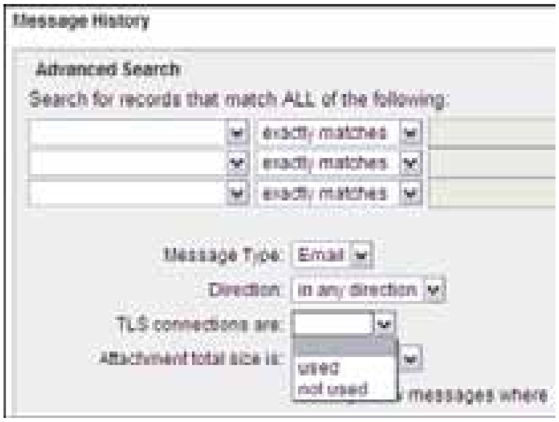
   Other TLS options are:

   - **Don't Use TLS** – TLS Mail Delivery is never used with the specified server.
   - **May Use TLS** – Use TLS if the specified server supports it.
   - **Enforce TLS** – Deliver to the specified server only if a TLS connection with a valid CA-signed certificate can be established.
   - **Loose TLS** – Similar to **Enforce TLS** but accepts a mismatch between the specified server name and the Common Name in the certificate.

2. In the **Add/Update Site** text box, type the IP Address or FQDN (Fully Qualified Domain Name) of the remote mail server.
3. Click the **Update** button.
   The exempted mail server is listed under the Specific Site Policy.

TLS and Message History

You can filter the **Message History** log for SSL/TLS messages in the **Activity > History > Message History > Advanced** search menu.



Message History

Advanced Search

Search for records that match ALL of the following:

exactly matches

exactly matches

exactly matches

Message Type: Email

Direction: in any direction

TLS connections are:

used

not used

Attachment total size is:

messages where

Certificates

A valid SSL certificate is required to support the encryption services available on the WatchGuard XCS. The SSL encrypted channel from the server to the web browser (for example, when you use a URL that begins with HTTPS), requires a valid digital certificate. You can use self-signed certificates generated by the system, or import certificates purchased from commercial vendors, for example, VeriSign.

A certificate binds a domain name to an IP address by means of the cryptographic signature of a trusted party. The web browser warns you of invalid certificates that undermine secure, encrypted communications with a server.

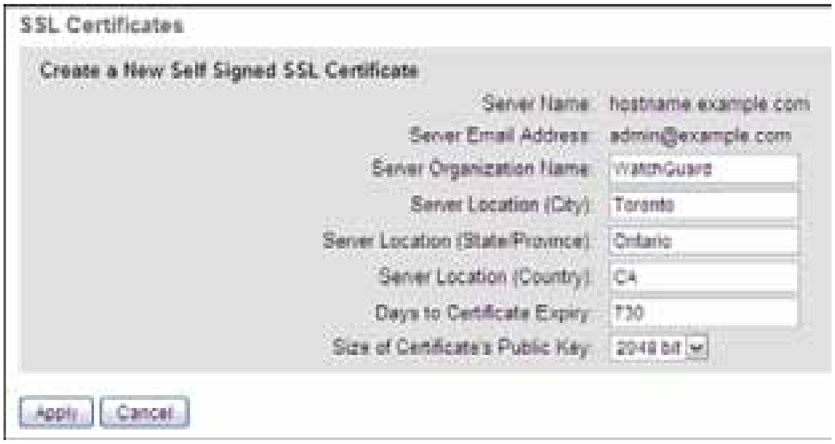
The disadvantage of self-signed certificates is that web browsers display warnings that the "company" (in this case, the WatchGuard XCS) issuing the certificate is untrusted. When you purchase a commercial certificate, the browser recognizes the company that signed the certificate and does not generate these warning messages.

A web server digital certificate can only contain one domain name, for example, server.example.com, and a limitation in the SSL protocol only allows one certificate per IP address. Some web browsers display a warning message when trying to connect to any domain on the server that has a different domain name than the server specified in the single certificate.

Digital certificates eventually expire and are no longer valid after a certain period of time and need to be renewed before the expiration date.

To install a commercial certificate:

1. Select **Administration > System > SSL Certificates**.
   The SSL Certificates page appears.
2. Click **Generate a 'self-signed' certificate**.



SSL Certificates

Create a New Self Signed SSL Certificate

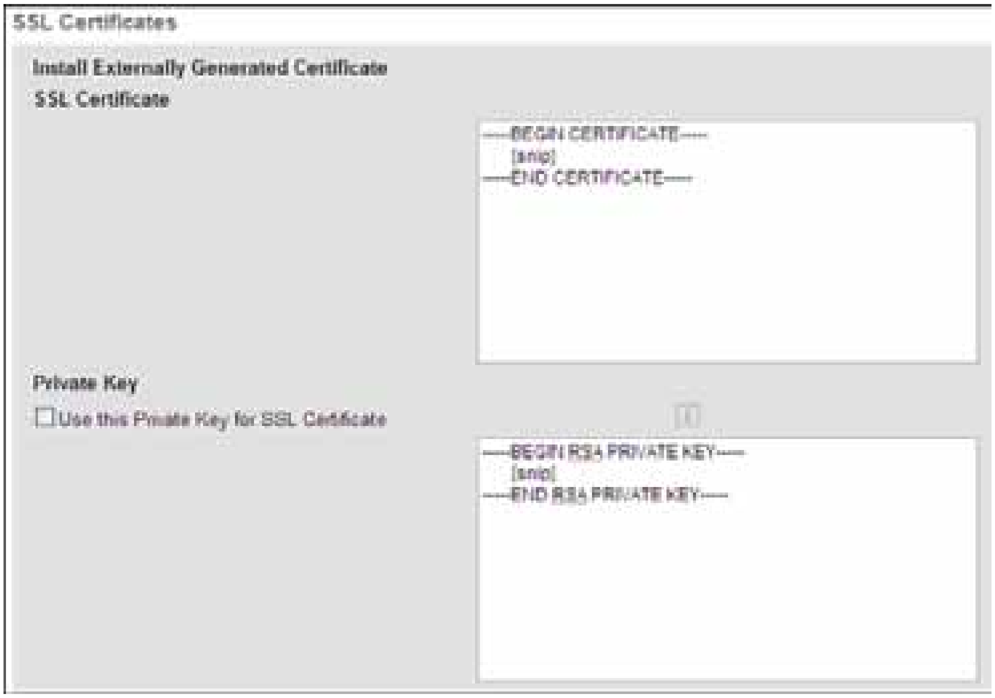
Server Name:	hostname.example.com
Server Email Address:	admin@example.com
Server Organization Name:	WatchGuard
Server Location (City):	Toronto
Server Location (State/Province):	Ontario
Server Location (Country):	CA
Days to Certificate Expiry:	730
Size of Certificate's Public Key:	2048 bit

3. Enter the required information for your organization in the form.
4. Click **Apply**.
   You must restart the system to install the certificate.

   After the system restarts, the current certificate and certificate request that was signed by the on-board Certificate Authority is displayed. To obtain a commercial certificate, send this certificate request information to the commercial Certificate Authority (CA) of your choice (for example, VeriSign or Entrust) for signing.

   > ***Note*** *Make sure that the certificate is an Apache type of certificate for a mail server.*

5. When you receive the certificate from the CA, click the **Load site certificate** button.



SSL Certificates

Install Externally Generated Certificate

SSL Certificate

```
-----BEGIN CERTIFICATE-----
    [snip]
-----END CERTIFICATE-----
```

Private Key

□ Use this Private Key for SSL Certificate

```
-----BEGIN RSA PRIVATE KEY-----
    [snip]
-----END RSA PRIVATE KEY-----
```

6. Copy and paste the PEM encoded certificate information from the signed SSL certificate returned by the CA into the **SSL Certificate** text box.
7. To use a supplied private key, select the **Use this Private Key for SSL Certificate** check box.
8. Copy and paste the PEM encoded private key into the **Private Key** text box.
   Do not enable this option and leave the field blank if the certificate was generated by a request from this WatchGuard XCS.

> ***Note*** *If you generate a new self-signed certificate after you install a commercial certificate, this action overwrites the private key associated with the installed commercial certificate and renders it invalid.*

9. Some commercial certificates require you to upload an intermediate certificate in addition to the commercial certificate and the private key. You can enter this information into the **Intermediate Certificate** section.

9 Content Control

Attachment Control

Attachment Control is used to control a wide range of problems originating from both inbound and outbound attachments in email messages and web requests:

- **Viruses and Spyware** – Blocks attachments and downloads carrying viruses, spyware, and other types of malware.
- **Offensive Content** – Blocks the transfer of images which reduces the possibility that an offensive picture is transmitted to or from your organization’s messaging and web systems.
- **Confidentiality** – Prevents the transmission of unauthorized documents through the WatchGuard XCS.
- **Loss of Productivity** – Prevents employee abuse of your organization’s computer resources.

In policies, you can set mail and web actions for both inbound and outbound Attachment Control. In addition, you can configure separate types of Attachment Control file and MIME type lists for email and web traffic.

Attachment Stripping

The Attachment Control feature can identify and remove attachments from inbound and outbound mail messages. You can configure a list of specific attachment extensions or MIME types that are stripped from a message before delivery. A configurable notification text attachment replaces the removed attachment that indicates to the user that the attachment is stripped and specifies the reason why it was removed.

> **Note** *Attachment Stripping is a global feature, and cannot be configured on a per-policy basis.*

The WatchGuard XCS determines the file extension and MIME-type for each MIME part in a message. If the file extension or MIME type exists in the Attachment Stripping global list, that specific file or MIME part is stripped from the message and discarded before delivery to the recipient. The attachment cannot be retrieved after it has been stripped from a message. The WatchGuard XCS also examines MIME parts contained in archive file types, for example, .zip. If a file to be stripped is found in an archive file, the entire archive file is stripped.

> **Note** *You must enable Kaspersky Anti-Virus to expand and examine archive files for attachments.*

Attachment stripping actions are performed in addition to any other scanning actions on a message, for example, Anti-Spam or content controls. A message can still be rejected or quarantined by other message scanners after the attachment is stripped. Any message encryption is performed after the attachments are stripped.

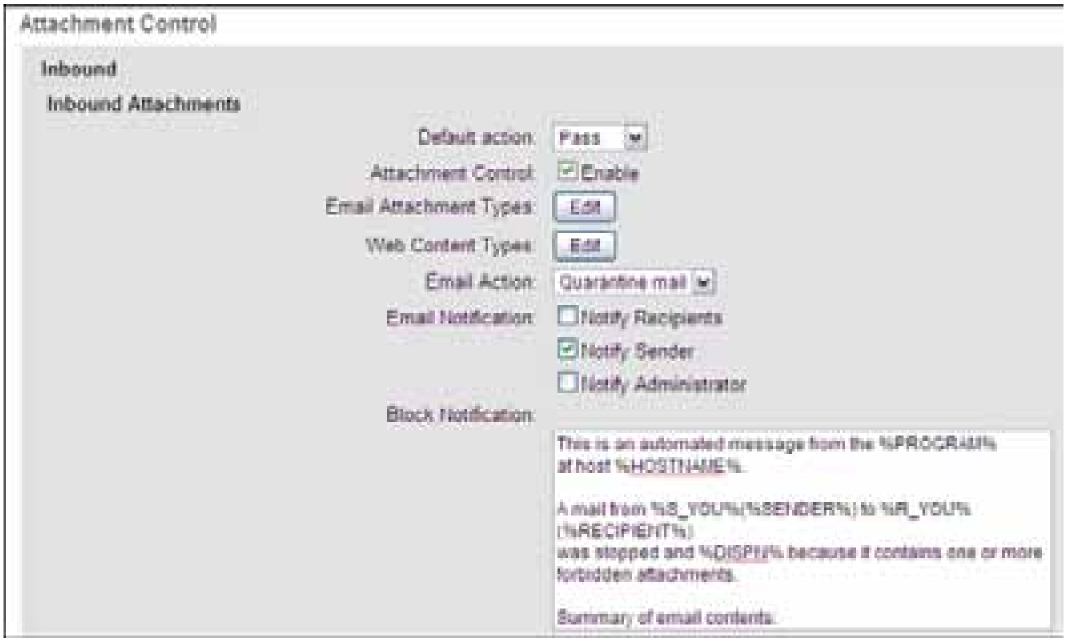
Attachment Stripping and DomainKeys Signatures

Attachment stripping is performed after the DomainKeys signature verification of inbound messages. This may invalidate DomainKeys message signatures for further recipients because the system modifies the message body. The WatchGuard XCS verifies any DomainKeys signatures before stripping attachments, but the signature is not valid for the final recipient because the message has been altered by the system to remove the attachments.

Configure Attachment Control

To configure Attachment Control:

1. Select **Security > Content Control > Attachment Control**.
   The Attachment Control page appears.



Attachment Control

Inbound

Inbound Attachments

Default action: Pass

Attachment Control: ☑ Enable

Email Attachment Types: Edit

Web Content Types: Edit

Email Action: Quarantine mail

Email Notification: ☐ Notify Recipients
☑ Notify Sender
☐ Notify Administrator

Block Notification:

This is an automated message from the %PROGRAM%
at host %HOSTNAME%.

A mail from %S_YOU%(%SENDER%) to %R_YOU%
(%RECIPIENT%)
was stopped and %DISP%% because it contains one or more forbidden attachments.

Summary of email contents.

2. From the **Default Action** drop-down list, select the action to perform for items not specifically listed in the *Attachment Types* list or attachments that cannot be identified.

   The default action is **Pass**, which allows all attachments. Any file types defined in the Attachment Types list override the default setting. The **Strip** action cannot be set as the default action, and can only be set within the Attachment Types list for mail messages.

   Select **Block** to block any attachment not listed in the Attachment Types list or attachments that cannot be identified.

> ***Note*** *If you use Attachment Control with Web content, setting a "Reject" HTTP action for blocked image types and other web file types effectively stops many web sites from working properly because files required for viewing of the web site are blocked.*

3. Select the **Attachment Control** check box.
   You can enable or disable Attachment Control independently for inbound and outbound messages.
4. For **Email Attachment Types**, click **Edit** to configure the action for each email attachment type.
5. For **Web Content Types**, click **Edit** to configure the action for each web content file type.
   The Web Proxy uses the HTTP Content Header to determine the MIME type of the file. Do not configure file extension in the Web Content Types.
6. From the **Email Action** drop-down list, select an action to perform:

   - **Just log** – Log the event and take no further action.
   - **Reject mail** – Reject the message and send a notification to the sending system.
   - **Quarantine mail** – Place the message into the administrative quarantine area. This is the default action.
   - **Discard mail** – Discard the message and do not send a notification to the sending system.

5. Select who to send notifications to when a message is caught by Attachment Control.

   You can select **Notify Recipient**, **Notify Sender**, or **Notify Administrator**, and customize the notification text.

6. In the **Stripped Attachment Text** text box, you can customize the text that replaces stripped attachments.

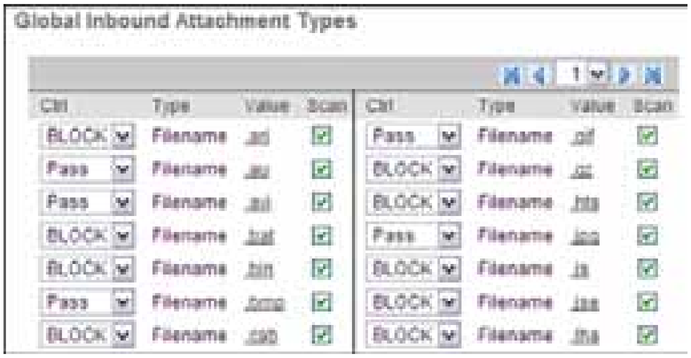
   The replacement text attachment uses the content type of "text/plain" and the US-ASCII character set.

> ***Note*** *Attachment Control actions for web content must be set in a policy. You can set email attachment control actions globally and within a policy.*

Edit Attachment Types

To edit attachment types:

1. For **Email Attachment Types** and **Web Content Types**, click **Edit** to edit your attachment and content types for email and web.



Global Inbound Attachment Types

Ctrl	Type	Value	Scan	Ctrl	Type	Value	Scan
BLOCK	Filename	.ani	☑	Pass	Filename	.pif	☑
Pass	Filename	.au	☑	BLOCK	Filename	.cc	☑
Pass	Filename	.avi	☑	BLOCK	Filename	.hta	☑
BLOCK	Filename	.bat	☑	Pass	Filename	.jpg	☑
BLOCK	Filename	.bin	☑	BLOCK	Filename	.js	☑
Pass	Filename	.bmp	☑	BLOCK	Filename	.jse	☑
BLOCK	Filename	.cab	☑	BLOCK	Filename	.lha	☑

2. For each attachment type, from the **Ctrl** drop-down list, select **Pass**, **Strip** (for mail messages only), or **BLOCK**.

   For attachments with no specified extension, there is a file type called **[no extension]** that is set to a default action of **Pass**.

3. Select the **Scan** check box to enable deep scanning for the selected extension or MIME type.

   The WatchGuard XCS can scan files within an archive file (for example, .zip) for forbidden attachments. If an archive file, for example, .zip, contains a file type that is blocked, the archive file is blocked, even if it is set to **Pass**. Clear the **Scan** check box if you do not want to scan the content of the specific archive file type. Virus scanning is still performed on the file.

> ***Note*** *You must enable Anti-Virus scanning to decompress archive files and check for forbidden attachments.*

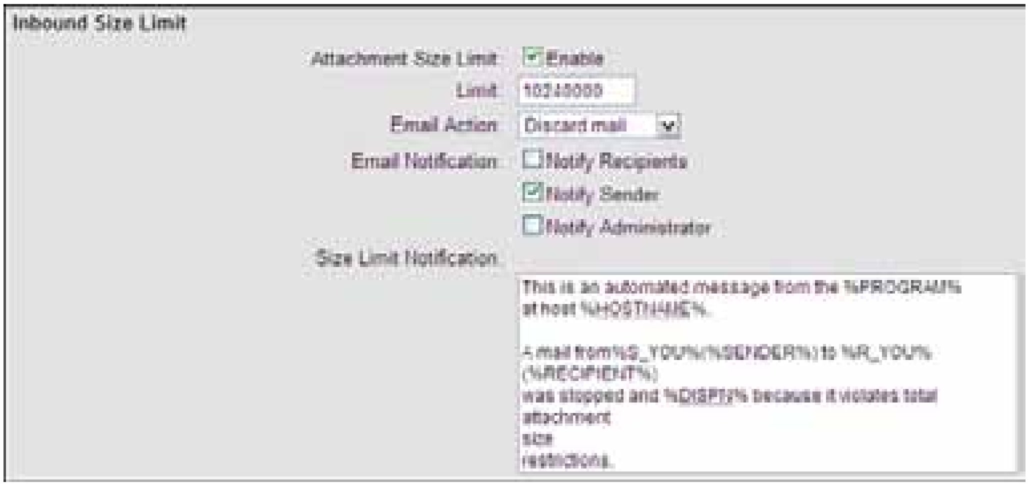
Attachment Size Limits

The Attachment Control feature can filter inbound and outbound mail messages based on the size of their attachments. You can set a size limit threshold that triggers an action if it is exceeded. If there is more than one attachment to the message, the attachment sizes are added together. You can configure attachment size limits globally and through policies.

> ***Note*** *Attachment size limits are checked before any other attachment control function, and size limit actions take precedence over attachment control actions.*

To configure attachment size limits:

1. Select **Security > Content Control > Attachment Control**.
2. Go to the **Inbound Size Limit** or **Outbound Size Limit** section.



Inbound Size Limit

Attachment Size Limit: ☑ Enable

Limit: 10240000

Email Action: Discard mail

Email Notification: □ Notify Recipients
☑ Notify Sender
□ Notify Administrator

Size Limit Notification:

```
This is an automated message from the %PROGRAM%
at host %HOSTNAME%.

A mail from%S_YOU%(%SENDER%) to %R_YOU%
(%RECIPIENT%)
was stopped and %DISP1% because it violates total
attachment
size
restrictions.
```

3. Select the **Attachment Size Limit** check box.
4. In the Limit text box, type the maximum attachment size (in bytes).

   Attachments greater than this threshold trigger the **Email Action** defined in the next step. The default is 10240000 bytes. Set to 0 to indicate no size limit.

   The **Maximum Message Size** configured in **Configuration > Mail > Access** is also set to 10240000 bytes, and this threshold is exceeded if the attachment size is close to the attachment size limit. We recommend that the **Maximum Message Size** value be at least 1.5 times the value of the **Attachment Size Limit** option to make sure that large attachments do not exceed the **Maximum Message Size**.

5. From the **Email Action** drop down list, select an action to perform on an email message when the attachment size threshold limit is exceeded:

   - **Just log** – Log the event and take no further action.
   - **Reject mail** – Reject the message and send a notification to the sending system.
   - **Quarantine mail** –Place the message into the administrative quarantine area.
   - **Discard mail** – Discard the message and do not send a notification to the sending system.

5. Select who to send notifications to when an attachment exceeds the size limit.

   You can select **Notify Recipient**, **Notify Sender**, or **Notify Administrator**, and customize the notification text.

6. Click **Apply**.

Content Scanning

Content Scanning performs deep scanning of attachments in email messages and web requests, for example, PDF and Microsoft document files, for patterns of text and phrases. This allows organizations to use filter rules and policy settings to scan attachments for specific content that could be considered offensive, private and confidential, or against existing compliance rules.

If you enable Content Scanning globally, no additional message processing occurs until you configure additional features to use the Content Scanning feature.

There are two methods for scanning the content of messages and attachments:

- Configure a Pattern Filter with the “Content Scanning” message part to search for text and phrases in a document.
- Use a dictionary with a policy to scan extracted message text and attachments for words and phrases that appear in the dictionary.

Unopenable Attachments

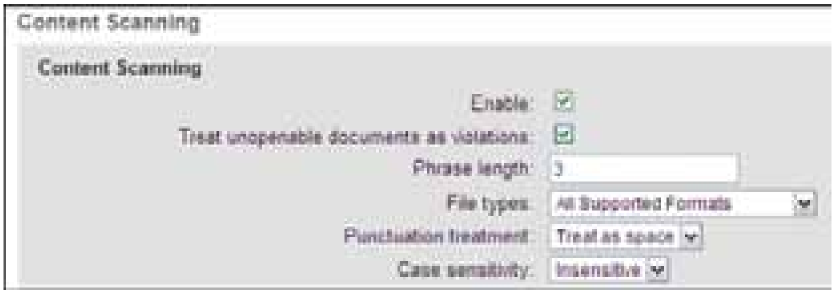
These cases of unopenable documents classifies the attachment as a compliance violation if you enable the **Treat unopenable documents as compliancy violations** option.

- Files larger than 1 GB
- File types not recognized by the scanner
- Files that take longer than one minute to scan
- Malformed or virus-infected attachments

Configuring Content Scanning

To configure Content Scanning:

1. Select **Security > Content Control > Content Scanning**.
   The Content Scanning page appears.



Content Scanning

Content Scanning

Enable: ☑

Treat unopenable documents as violations: ☑

Phrase length: 3

File types: All Supported Formats

Punctuation treatment: Treat as space

Case sensitivity: Insensitive

2. Select the **Enable** check box.
3. To treat unopenable documents as though they were not compliant, select the **Treat unopenable documents as violations** check box.
   Attachments that are protected by a password or encrypted can contain text that is a compliance violation.
4. In the **Phrase Length** text box, type the phrase length to use for pattern-matching checks.
   This number of words is passed to the scanning engine to check if it matches any phrases in your compliance file.

> ***Note*** *Long phrases result in greater processing times. We recommend that phrases be five words or less. The phrase length of the compliance dictionary selected for Content Scanning must not be greater than the phrase length selected in this text box. A phrase length of at least four must be used with the default Financial and Medical dictionaries and Credit Card pattern filters.*

5. From the **File Types** drop-down list, select the types of files to scan:
   - **All Supported Formats**– Scans all file formats supported by the content scanner.
   - **Common Document Formats**– Scans only common word processing, spreadsheet, database, presentation, text, and archive formats.

- **Standard Document Formats**– Scans only common document formats (word processing, spreadsheet, database, presentation, text, and archive files). This includes less common formats, for example, graphics and desktop publishing formats.

6. From the **Punctuation Treatment** drop-down list, select how to treat punctuation in words and phrases:
    - **Significant**– The punctuation is considered as part of the word or phrase it appears in.
    - **Treat as space**– The punctuation is treated as a space. For example, the phrase “This, is classified” is treated as “This is classified”. This is the default setting.
    - **Ignore**– The punctuation is completely ignored.
7. From the **Case Sensitivity** drop-down list, select how the scanning engine treats capitalization.

    The default is **Insensitive**. Select **Sensitive** to take capitalization of letters into account. For example, the word “Classified” must appear in the phrase compliance file with the first letter capitalized.
8. Select who to send notifications to when a message is caught by Content Scanning.

    You can select **Notify Recipient**, **Notify Sender**, or **Notify Administrator**, and customize the notification text.
9. Click **Apply**.

Use Pattern Filters for Content Scanning

To create a Pattern Filter for use with Content Scanning:

1. Select **Security** > **Content Control > Pattern Filters**.
2. Click **Add**.
3. From the **Apply To** drop-down list, select whether you want to check **Inbound**, **Outbound**, or **All Mail**.
4. From the **Message Part** drop-down list, select **Content Scanning**.

> ***Note*** *Content Scanning scans the entire email message. This includes the header, body and any attachment for matching content.*

5. In the **Pattern** text box, enter a text pattern to match against.
6. From the **Action** drop-down list, select an action to perform on a message that contains the pattern text, for example, **Reject**.
7. Click **Apply**.

Use a Compliance Dictionary for Content Scanning

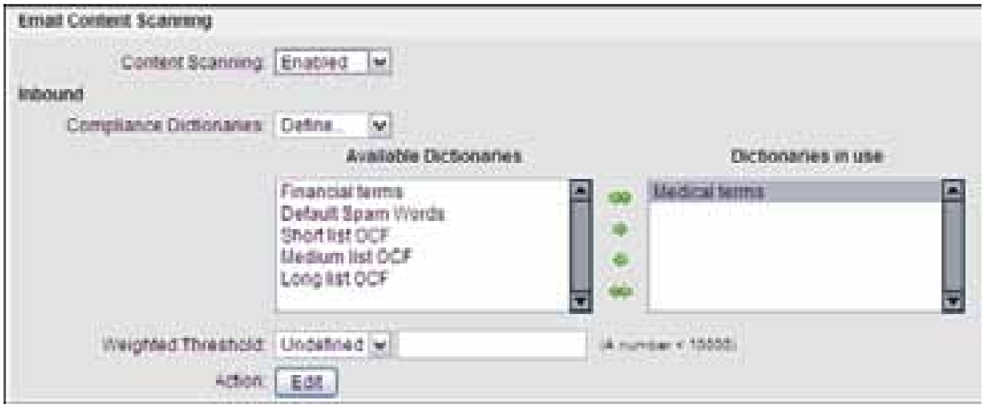
You can also perform Content scanning with policies by uploading compliance dictionaries. The compliance dictionaries contain a list of words and phrases that are checked against text in scanned attachment files and web uploads and downloads.

You can set a weighted threshold for weighted compliance dictionaries. For example, the system can encrypt an outbound message when the phrase “patient number” and the term “diagnosis” is detected in the same message content. In the weighted dictionary, these terms can be configured to have a weight of

50. If the weighted threshold for the compliance dictionary is set to 100, these two terms, or any number of terms that match or exceed a weight of 100, result in the message being encrypted. In the specified Content Control policy, select the dictionaries to use with the policy. If required, select a weighted threshold between 1 and 9999.

To configure a compliance dictionary to use for Content Scanning:

1. Select **Security > Policies > Policies**.
2. Select an existing policy or add a new policy.
3. Select **Content Control**.
4. In the **Email Content Scanning** section, from the **Compliance Dictionaries** drop-down list, select **Define**.



Email Content Scanning

Content Scanning: Enabled

Inbound

Compliance Dictionaries: Define...

Available Dictionaries: Financial terms, Default Spam Words, Short list OCF, Medium list OCF, Long list OCF

Dictionaries in use: Medical terms

Weighted Threshold: Undefined (A number < 10000)

Action: Edit

5. Use the arrow buttons to move a dictionary from the **Available Dictionaries** section to the **Dictionaries in Use** section.

   To upload custom dictionary files, select **Security > Content Control > Dictionaries & Lists**.

   See *Dictionaries and Lists* for more detailed information on uploading custom dictionary files.
6. From the **Weighted Threshold** drop-down list, select **Define** to enter an optional weighted threshold for the dictionary.
7. In the **Action** field, click **Edit** to select the corresponding action to perform for Email and HTTP traffic, for example, **Reject**, and select the notifications to send.
8. Click **Apply**.

Objectionable Content Filter

The *Objectionable Content Filter* (OCF) defines a list of key words that cause a message to be blocked if any of those words appear in the message. The Objectionable Content Filter provides enhanced content filtering functionality and flexibility, allowing users to restrict objectionable words and phrases, and offensive content.

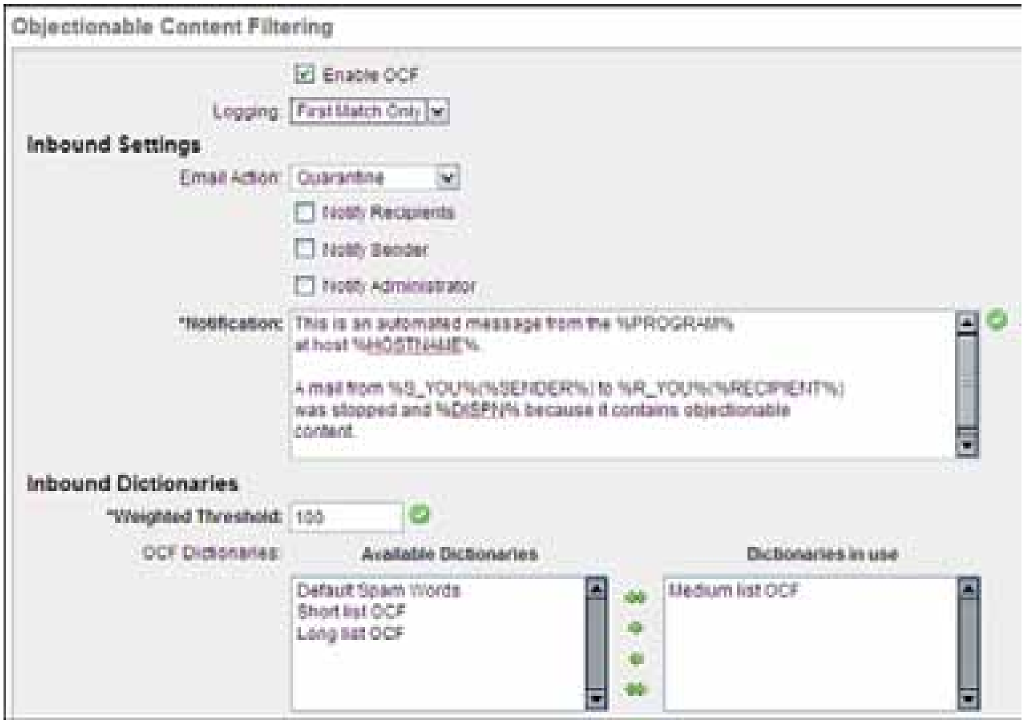
The predefined lists provided are configurable and can be updated and customized to meet the specific needs of any organization. Rules can also be applied to both inbound and outbound email messages and web uploads and downloads. This prevents unwanted content from entering an organization, and prohibits the release of sensitive content outside an organization.

OCF words are extracted from messages that disguise the words with certain techniques. For example, OCF detects the word “spam”, even if it is disguised as “sp@m” or “s_p_a_m” using the advanced token recognition component of the Token Analysis feature.

> ***Note*** *OCF has a maximum of 35 characters for a word. OCF does not detect plurals of words. Both plural and singular word forms must be defined in the dictionaries.*

To configure OCF:

1. Select **Security > Content Control > Objectionable Content**.



Objectionable Content Filtering

☑ Enable OCF

Logging: First Match Only

Inbound Settings

Email Action: Quarantine

□ Notify Recipients

□ Notify Sender

□ Notify Administrator

*Notification: This is an automated message from the %PROGRAM% at host %HOSTNAME%.

A mail from %S_YOU%(%SENDER%) to %R_YOU%(%RECIPIENT%) was stopped and %DISPN% because it contains objectionable content.

Inbound Dictionaries

*Weighted Threshold: 100

OCF Dictionaries:

Available Dictionaries: Default Spam Words, Short list OCF, Long list OCF

Dictionaries in use: Medium list OCF

2. Select the **Enable OCF** check box.
3. From the **Logging** drop-down list, select the type of logging to perform for OCF processing:

   - **No Logging** – Do not log OCF actions.
   - **First match only** – Log the first word that is matched by the filter.
   - **All matches** – Log all words that are matched by the filter.
   - From the **Email Action** drop-down list, select an action to perform:
   - **Just log** – Log the event and take no further action.
   - **Reject mail** – Reject the message and send a notification to the sending system.
   - **Quarantine mail** – Place the message into the administrative quarantine area.
   - **Discard mail** – Discard the message and do not send a notification to the sending system.
   - **Encrypt** – Redirect the message to an encryption server.
   - **Decrypt** – Redirect the message to a decryption server.
   - **Archive** – Redirect the message to an archive server.
   - **SecureMail Encrypt** – Encrypts the message with the integrated SecureMail encryption engine.
   - **PostX Encrypt** – Encrypt the message with the integrated PostX encryption engine.

4. In the **Weighted Threshold** text box, type a threshold for OCF to classify a message as containing objectionable content. This threshold only applies if you use weighted dictionaries.You can specify a value between 1 and 9999. The default is 100.

   If the aggregate weight of the OCF words found in a message matches or exceeds this threshold, OCF performs the configured action. If both weighted and unweighted dictionaries are used, the final action is triggered if the sum of the weights exceeds the configured weighted threshold, or if a match occurs in an unweighted dictionary.

5. Select the **OCF Dictionaries** to use with inbound and outbound OCF.

   The dictionaries available are listed in the **Available Dictionaries** section. Use the arrow buttons to move the dictionaries to the **Dictionaries in Use** section as required.

   The default OCF dictionaries consist of a “Short”, “Medium”, and “Long” list of common objectionable words and phrases. You can create your own OCF dictionary files in **Security > Content Control > Dictionaries & Lists**.

   > ***Note*** *The OCF dictionaries contain content that are of a vulgar nature. The pre-defined dictionaries must be viewed with caution because they contain words and phrases that are offensive. All dictionaries must be reviewed and modified as required before you enable them for use with OCF.*

6. Select who to send notifications to when a message is caught by OCF.

   You can select **Notify Recipient**, **Notify Sender**, or **Notify Administrator**, and customize the notification text.

7. Click **Apply**.

Document Fingerprinting

Document Fingerprinting scans trusted, outbound email messages and their attachments, and allows or blocks the delivery of these messages as required by comparing them to an uploaded training set of allowed and forbidden documents.

> ***Note*** *Document Fingerprinting only scans outbound messages relayed from a trusted source.*
> *An outbound message that matches an “Allow Relaying” Specific Access Pattern is not scanned by Document Fingerprinting.*

Document Fingerprinting extracts text from common office document formats, for example, plain text, HTML, PDF, and Microsoft Office (Word, Excel, Powerpoint). This text is compared to the existing document training set uploaded by the administrator. The outbound message is assigned a score (between 0 and 100) that indicates to which category it belongs. A score closer to 0 indicates an allowed category. A score closer to 100 indicates the forbidden category.

> ***Note*** *Content Scanning must be enabled to scan common office document file types, for example, Microsoft Office and PDF formats with Document Fingerprinting.*

If the Document Fingerprinting score is greater than the configured threshold, the document is classified as forbidden, and the specified action is performed on the message. For example, if the administrator sets the threshold to 90, any scanned message with a Document Fingerprinting score of 90 or greater is considered as forbidden and the configured action is performed on the message.

Upload Training Documents

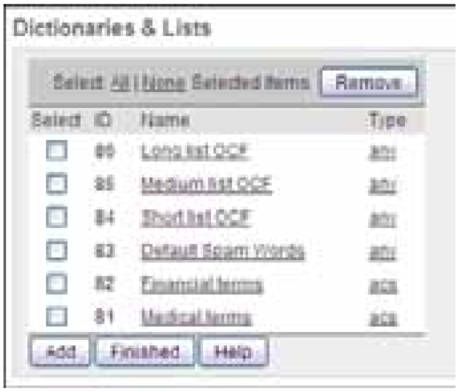
Before you enable Document Fingerprinting, you must upload at least one allowed and one forbidden document for training purposes. You can upload documents one at a time, or you can upload an archive file (of .zip or .gzip format) containing several documents for each category.

The WatchGuard XCS assumes that all data in plain text and HTML message parts belong to the ISO-8859-1 character set. Text extracted from other types of documents, for example, Microsoft Office files, are converted to the ISO-8859-1 character set. Any characters that do not exist in the ISO-8859-1 characters set are converted to the “*” character.

> **Note** *You can only upload training documents on a global basis. You cannot upload different training sets within policies.*

To upload training documents:

1. Select **Security > Content Control > Dictionaries and Lists**.
   The Dictionaries & Lists page appears.

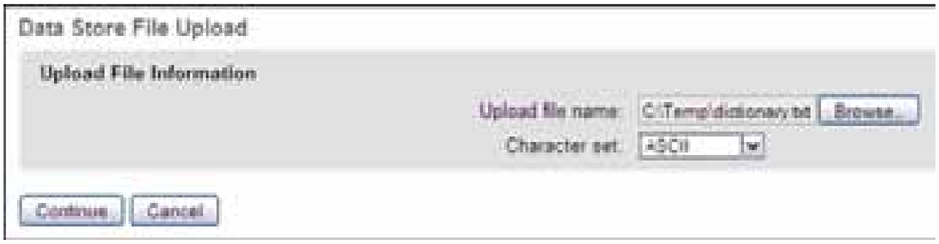


Dictionaries & Lists

Select: All | None Selected Items

Select	ID	Name	Type
□	86	Long list OCF	any
□	85	Medium list OCF	any
□	84	Short list OCF	any
□	83	Default Spam Words	any
□	82	Financial terms	acs
□	81	Medical terms	acs

2. Click **Add**.

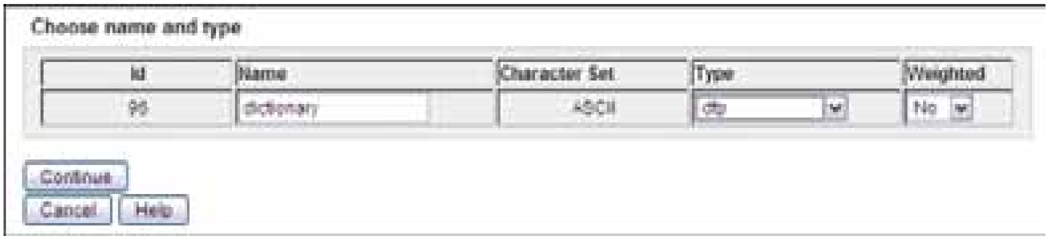


Data Store File Upload

Upload File Information

Upload file name: C:\Temp\dictionary.txt
Character set: ASCII

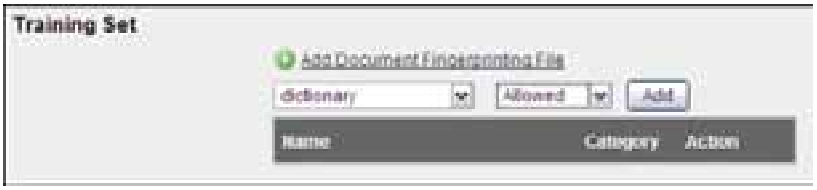
3. Click **Browse** and select the file to upload.
4. From the **Character Set** drop-down list, select the correct character set for the content.
   Choose the BINARY character set if you upload a Microsoft Office, PDF file, or .zip archive of documents.



Choose name and type

Id	Name	Character Set	Type	Weighted
96	dictionary	ASCII	dfp	No

5. From the **Type** drop-down list, select **dfp**.
6. Click **Continue**.
7. Select **Security > Content Control > Document Fingerprinting**.



Training Set

Add Document Fingerprinting File

dictionary | Allowed | Add

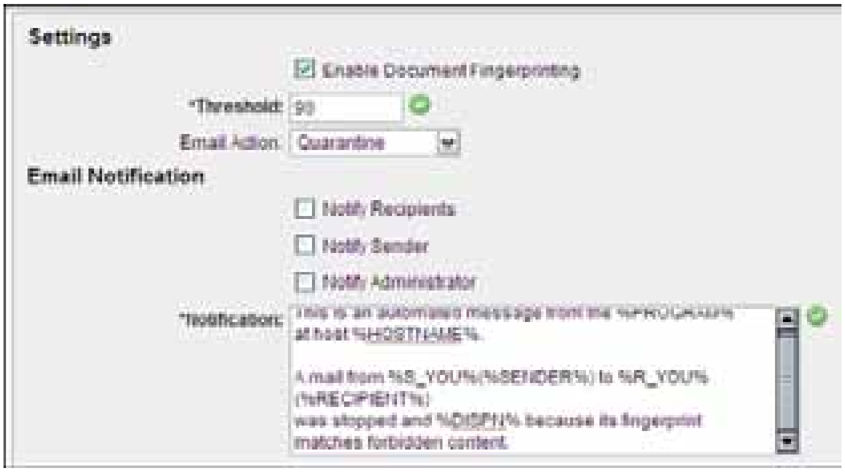
Name	Category	Action

8. In the **Training Set** section, click **Add Document Fingerprinting File**.
9. From the file drop-down list, select the existing document file.
10. From the adjacent drop-down list, select if this file is **Allowed** or **Forbidden**.
11. Click **Add**.

Configure Document Fingerprinting

To configure Document Fingerprinting:

1. Select **Security > Content Control > Document Fingerprinting**.
   The Document Fingerprinting page appears.



Settings

☑ Enable Document Fingerprinting

*Threshold: 90

Email Action: Quarantine

Email Notification

☐ Notify Recipients

☐ Notify Sender

☐ Notify Administrator

*Notification:

```
This is an automated message from the %PROGRAM%
at host %HOSTNAME%.

A mail from %S_YOU%(%SENDER%) to %R_YOU%
(%RECIPIENT%)
was stopped and %DISPN% because its fingerprint
matches forbidden content.
```

2. Select the **Enable Document Fingerprinting** check box.

> **Note** *You cannot enable Document Fingerprinting until you upload at least one allowed file and one forbidden file for training.*

3. In the **Threshold** text box, type a Document Fingerprinting threshold between 0 and 100.

   Scores closer to 0 indicate the allowed category. Scores closer to 100 indicate the forbidden category. The default threshold is 90. Any scanned message with a score of 90 or greater triggers the specified action.

4. From the **Email Action** drop-down list, select an action to perform on the message when the Document Fingerprinting threshold is exceeded.

   - **Just log** – Log the event and take no further action.
   - **Reject mail** – Reject the message and send a notification to the sending system.
   - **Quarantine mail** – Place the message into the administrative quarantine area.
   - **Discard mail** – Discard the message and do not send a notification to the sending system.
   - **BCC** – Send a Blind Carbon Copy of the message to the specified email address.
   - **Encrypt** – Redirect the message to an encryption server.
   - **Decrypt** – Redirect the message to a decryption server.
   - **Archive** – Redirect the message to an archive server. Archive priority can be set to **Low**, **Medium**, and **High**.
   - **SecureMail encrypt** – Encrypts the message with the integrated SecureMail encryption engine.
   - **PostX Encrypt** – Encrypt the message with the integrated PostX encryption engine.

5. Select who to send notifications to when a message is caught by Document Fingerprinting.

   You can select **Notify Recipient**, **Notify Sender**, or **Notify Administrator**, and customize the notification text.

6. To include Document Fingerprinting diagnostic headers in the message header, select the **Enable Diagnostic Headers** check box.

   The Document Fingerprinting message score and highest and lowest token scores are helpful in troubleshooting message delivery issues.

7. Click **Apply**.

Pattern Filters

Pattern Filters are the primary tool for creating filter rules on the WatchGuard XCS. Pattern Filters are used for:

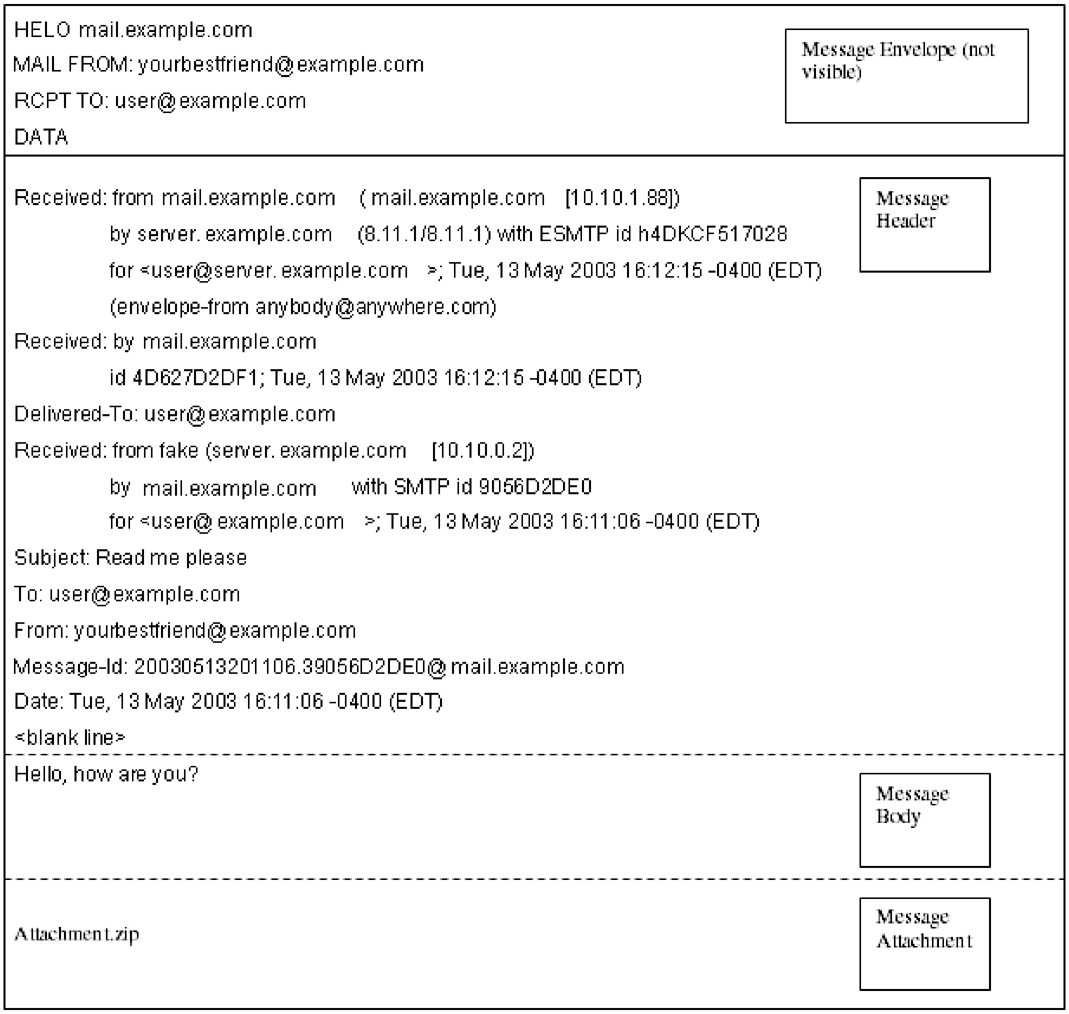
- Trusting and blocking messages containing certain text or characteristics
- Creating content filter rules for managing email messages

An administrator can create filter rules for any aspect of an email message. This includes the message header, sender, recipient, subject, attachment content, and message body text. For example, administrators can create a simple text filter that specifies to check messages for the word “spam” in the subject. This filter rule is helpful in correcting disadvantages in the other spam filters.

> ***Note*** *Specific Access Patterns must be used to trust specific servers because Pattern Filters can bypass or interfere with certain content filters, for example, Content Scanning and OCF, that occur later in the processing order.*

Email Message Structure

This is an example of a typical mail message:



```
HELO mail.example.com
MAIL FROM: yourbestfriend@example.com
RCPT TO: user@example.com
DATA
Received: from mail.example.com   ( mail.example.com   [10.10.1.88])
          by server. example.com   (8.11.1/8.11.1) with ESMTP id h4DKCF517028
          for <user@server. example.com   >; Tue, 13 May 2003 16:12:15 -0400 (EDT)
          (envelope-from anybody@anywhere.com)
Received: by mail.example.com
          id 4D627D2DF1; Tue, 13 May 2003 16:12:15 -0400 (EDT)
Delivered-To: user@example.com
Received: from fake (server. example.com   [10.10.0.2])
          by  mail.example.com     with SMTP id 9056D2DE0
          for <user@ example.com   >; Tue, 13 May 2003 16:11:06 -0400 (EDT)
Subject: Read me please
To: user@example.com
From: yourbestfriend@example.com
Message-Id: 20030513201106.39056D2DE0@ mail.example.com
Date: Tue, 13 May 2003 16:11:06 -0400 (EDT)
<blank line>
Hello, how are you?

Attachment.zip
```

Message Envelope

The information in the message envelope (HELO, MAIL FROM, and RCPT TO) are parameters not visible to the user. They are the handshake part of the SMTP protocol. You need to look for these in the log files or have other knowledge of them.

Message Header

The message header includes these fields:

Received from

Indicates the final path that the message followed to get to its destination. It arrived from mail.example.com, which delivered it to server.example.com to be put in the mailbox of user@server.example.com.

Received by

This indicates a previous hop that the message followed. In this case, the message came through mail.example.com which accepted the message addressed to user@example.com.

Delivered-To

The user to which to deliver to, in this example, user@example.com.

Received from

This field marks the origin of the message. Note that it is not necessarily the same as the actual server that sent the message.

Subject

This is a free form field and is displayed by a typical mail client.

To

This is a free form field and is displayed by a typical mail client. It may be different from the destination address in the Received headers or from the actual recipient.

From

This is a free form field and is displayed by a typical mail client. It may be different from the From address in the Received headers. It is typically faked by spammers.

Message-ID

This is added by the mail server and is often faked by spammers.

Other header fields include Reply-to, Sender, and others. These fields can be forged by spammers because they do not affect how the mail is delivered.

Message Body

After the header is the text or content of the message. This content can be formatted or encoded in many different ways, but in this example, it is displayed as plain text.

Message Attachment

Many emails contain attachments to the main message. The system has the ability to decode attachments to match text found within an attachment using a filter rule.

Default Pattern Filters

These default Pattern Filters support the user submitted "Spam" and "Not Spam" training feature:

- All Mail Envelope To: matches spam@mailsupport.watchguard.com (trains on user submitted spam messages)
- All Mail Envelope To: matches notspam@mailsupport.watchguard.com (trains on user submitted not spam messages)

The other predefined default pattern filters are included to make sure that mail is not trained in these situations:

- Outbound Mail To: contains @watchguard.com
- Outbound Mail To: contains @borderware.com
- All Mail Subject: contains [SPAM]
- All Mail Subject: contains [MAYBE SPAM]
- All Mail Subject: contains Spam summary for
- All Mail Subject: contains Delayed Mail
- All Mail Subject: contains Delivery Status Notification
- All Mail Subject: contains Delivery Failure Notification
- All Mail Subject: contains Undelivered Mail Returned to Sender
- All Mail Subject: contains AutoReply
- All Mail Subject: contains Returned Mail:
- All Mail From: contains postmaster@ + domain
- All Mail From: contains MAILER-DAEMON@ + domain

These rules help prevent misconfiguration of the Token Analysis database to make sure that forwarded spam messages, delivery notifications, automatic replies, and system messages are not trained.

> ***Note*** *Spam messages must never be forwarded within an organization because this action can misconfigure the Token Analysis training database.*

Additional postmaster and MAILER-DAEMON Pattern Filters must be created for organizations supporting multiple domains.

You can edit or remove the default Pattern Filter rules in **Security > Content Control > Pattern Filters**.

Credit Card Pattern Filters

To assist you with regulatory compliance for Payment Card Industry (PCI) and other types of Data Loss Prevention (DLP) digital security standards, the WatchGuard XCS includes predefined regular expression Pattern Filters that search messages and attachments for specific credit card patterns using the Content Scanning feature.

Several default credit card types are provided (Diners Club, American Express, Discover, MasterCard, and Visa) that allow you to search for these patterns in incoming and outgoing messages and attachments.

For example, any messages or attachments that contain a credit card number can be encrypted before delivery to protect the data.

By default, the credit card pattern filters are initially disabled and set to the action of **Just Log**.

To enable and edit the pattern filter:

1. Select the credit card Pattern Filter to edit.
2. Select the **Enabled** check box to enable the pattern filter.
3. From the **Action** drop-down list, select an action to take when this credit card pattern is detected in a message or attachment.

   For example, you can Encrypt a message before it is sent if a credit card pattern is detected.

Content Scanning Phrase Length for Credit Card Pattern Filters

The Content Scanning feature has a default phrase length of 3, indicating that the system only scans up to 3 words of a dictionary phrase. When you enable Credit Card patter filters, you must increase the phrase length to at least 4 to make sure the credit card filters are properly scanned.

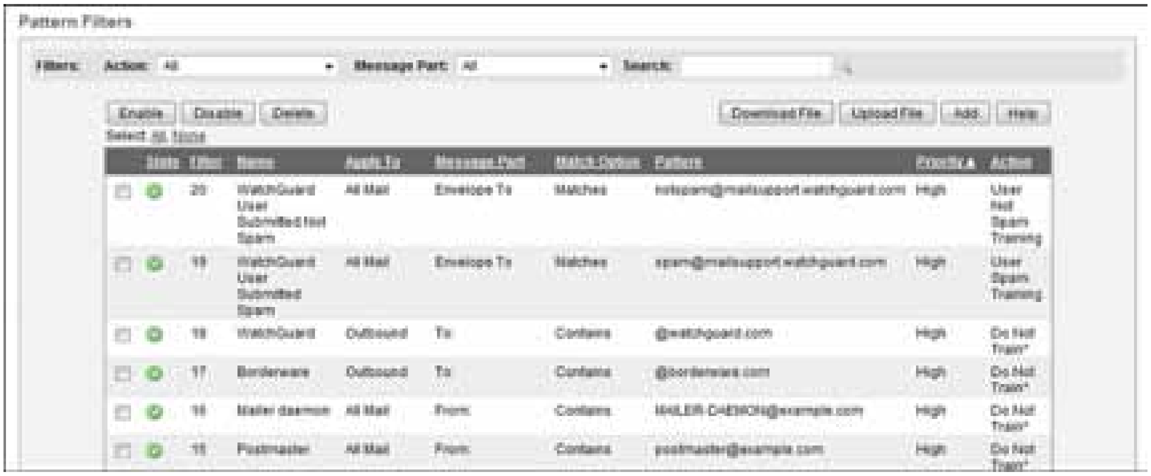
To modify the content scanning phrase length:

1. Select **Security > Content Control > Content Scanning**.
2. Select the **Enable** check box.
3. In the **Phrase Length** text box, type 4.
4. Click **Apply**.

Configure Pattern Filters

To configure Pattern Filters:

1. Select **Security > Content Control > Pattern Filters**.
   The Pattern Filters page appears.

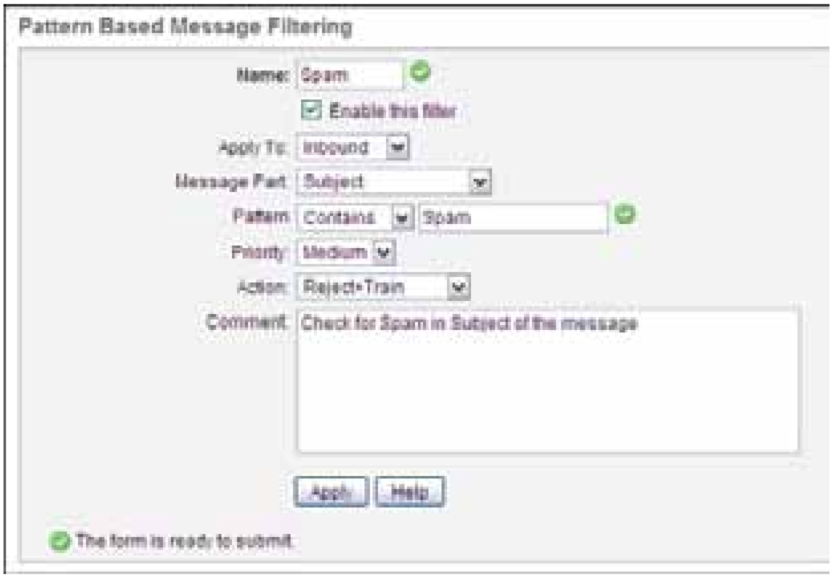


Pattern Filters

Filters: Action: All Message Part: All Search:

	State	Filter	Name	Apply To	Message Part	Match Option	Pattern	Priority ▲	Action
□	✓	20	WatchGuard User Submitted Not Spam	All Mail	Envelope To	Matches	notspam@mailsupport.watchguard.com	High	User Not Spam Training
□	✓	19	WatchGuard User Submitted Spam	All Mail	Envelope To	Matches	spam@mailsupport.watchguard.com	High	User Spam Training
□	✓	18	WatchGuard	Outbound	To	Contains	@watchguard.com	High	Do Not Train*
□	✓	17	Borderware	Outbound	To	Contains	@borderware.com	High	Do Not Train*
□	✓	16	Mailer daemon	All Mail	From	Contains	MAILER-DAEMON@example.com	High	Do Not Train*
□	✓	15	Postmaster	All Mail	From	Contains	postmaster@example.com	High	Do Not Train*

2. Click **Add**.



Pattern Based Message Filtering

Name: Spam

☑ Enable this filter

Apply To: Inbound

Message Part: Subject

Pattern: Contains | Spam

Priority: Medium

Action: Reject+Train

Comment: Check for Spam in Subject of the message

The form is ready to submit.

3. In the **Name** text box, type a name for this Pattern Filter.
   The name can only consist of letters, numbers, spaces, periods, underscores, and dashes.
4. Select the **Enable this filter** check box.
5. From the **Apply To** drop-down list, select the direction of mail for the Pattern Filter rule:

   - **All Mail** – Mail destined for any domain.
   - **Inbound** – Any mail that is destined to a domain for which the system is configured to accept mail for. This is any domain listed in the mail routing table in **Configuration > Mail > Routing**.
   - **Outbound** – Mail destined to any domain for which the system is not configured to accept mail (every domain other than those configured in Mail Routing).

6. From the **Message Part** drop-down list, select a message part on which to filter.

   These parameters are not visible to the user. They are the handshake part of the SMTP protocol. You can filter on these parameters.

   <<Mail Envelope>>

   This parameter allows for a match on any part of the message envelope which includes the HELO, Client IP, and Client Host.

   HELO

   This field is easily faked, and is not recommended for use in spam control. It may be useful in trusting a source of mail. For example: mail.example.com.

   Client IP

   This field is accurately reported and can be reliably used for both blocking and trusting. It is the IP address of the system initiating the SMTP connection. For example: 192.168.1.200.

   Client Host

   This field is accurately reported and can be reliably used for both blocking and trusting.
   For example: mail.example.com.

These envelope parameters (Envelope Addr, Envelope To, and Envelope From) may be visible if your client supports reading the message source. They can also be found in the transport logs. Other header fields may be visible as supported by the mail client.

Envelope Addr

This finds matches in either the Envelope To or Envelope From field. These fields are easily faked, and are not recommended for use in spam control. They may be useful in trusting a source of mail. For example: fred@example.com.

Envelope To

This field is easily faked, and is not recommended for use in spam control. It may be useful in trusting a source of mail. For example: fred@example.com.

Envelope From

This field is easily faked, and is not recommended for use in spam control. It may be useful in trusting a source of mail. For example: fred@example.com.

Message Header Parameters

Spammers typically enter false information into these fields, except for the Subject field, and they are usually not useful for controlling spam. These fields can be useful in trusting certain users or legitimate source of email.

> **Note** *Mail Header parameters only match on the primary header of a message and not other multi-part message headers.*

<<Mail Header>>

This parameter allows for a match in any part of the message header.

<<Recipient>>

This parameter finds matches in the To: or CC: fields of the message.

CC:

This parameter finds matches in the CC: (Carbon Copy) field of the message.

From:

This parameter finds matches in the From: field of the message.

Message-ID:

This parameter finds matches in the Message-ID: field of the message.

Received:

This parameter finds matches in the Received: field of the message.

Reply-to:

This parameter finds matches in the Reply-to: field of the message.

Sender:

This parameter finds matches in the Sender: field of the message.

Subject:

This parameter finds matches in the Subject: field of the message.

To:

This parameter finds matches in the To: field of the message.

There are other header fields that are commonly used, for example, List-ID, as well as those added by local mail systems and clients. You must use Regular Expressions to specify these parameters.

Message Body Parameters

<<Raw Mail Body>>

This parameter finds matches in any part of the encoded message body. This encoded content includes Base64, MIME, and HTML. Because messages are not decoded, a simple text match may not work. Use <<Mail Content>> for text matching on the decoded content. This parameter also matches in multi-part message parts.

<<Mail Content>>

This parameter finds matches in the visible decoded message body.

STA (Token Analysis) Token

Token Analysis tokens can also be selected for pattern based message filters. This allows you to match patterns for common spam words that can be hidden or disguised with fake or invisible HTML text comments, that would not be caught by a normal pattern filter. For example, Token Analysis extracts the token “viagra” from the text “vi<spam>ag<spam>ra” and “v.i.a.g.r.a.”.

Content Scanning

You can define Pattern Filters to match the content of an entire mail message and its attachments. This type of Pattern Filter is used with the Content Scanning feature.

7. From the **Pattern** drop-down list, select a matching option:
   - **Contains** – Looks for the text to be contained in a line or field. This allows for spaces or other characters that can make an exact match fail.
   - **Ends with** – Looks for the text at the end of the line or field (no characters, spaces and so on, between the text and the non-printed end-of-line character.)
   - **Matches** – The entire line or field must match the text.
   - **Starts with** – Looks for the text at the start of the line or field (no characters between the text and the start of line.)
   - **Reg Exp** – Enter a regular expression to match the text.
8. In the **Pattern** text box, type a text pattern (case insensitive) to search for in the message.

   You can also use regular expressions that allow you to specify match rules in a more flexible manner. Regular expressions are based on the standard POSIX specification for regular expressions.

   For example, to search for a blank message field, use this regular expression:

   ```
   ^subject:[[:blank:]]*$
   ```

> **Note** *WatchGuard cannot help with devising or debugging Regular Expressions because the expressions have an infinite variety and can be very complex. We recommend you do not use regular expressions unless you have advanced knowledge of their use.*

9. From the **Priority** drop-down list, select a priority for the Pattern Filter (**High**, **Medium**, **Low**).

   The entire message is read before a decision is made about which filter to use. If a message matches multiple filters, the filter with the highest priority is used. If more than one matched filter has the highest priority, the filter with the strongest action is used, in order, from highest priority to lowest (**Bypass**, **Reject**, **Discard**, **Quarantine**, **Certainly Spam**, **PostX Encrypt**, **Archive**, **Redirect**, **Trust**, **Relay**, **Accept**, **Just log**). Note that **Discard**, **Quarantine**, and **Redirect** are only available as custom actions.

   If more than one matched rule has the highest priority and highest action, then the filter with the highest rule number is used.

10. From the **Action** drop-down list, select an action to perform when Pattern Filter is matched:

    - **User Spam Train** – This action is used to train on spam messages submitted by end users.
    - **User Not Spam Train** – This action is used to train on legitimate (not spam) messages submitted by end users.

> **Note** *The User Spam Training and User Not Spam Training actions are used with the default Pattern Filters for user submitted messages.*

- **Bypass** – Allow this message to bypass all Intercept Anti-Spam and Content Control (Attachment Control, Content Scanning, Malformed Message, and OCF) processing. This action overrides other Pattern Filter actions for the same priority. This action does not bypass Anti-Virus scanning.
- **Trust** – This mail is considered trusted and from a legitimate source. This message is not processed for spam. Mail is trained as legitimate mail.
- **Reject** – Mail is received, then rejected before the close of an SMTP session. Message is trained for spam if **Train** is also selected.
- **Relay** – Message can be relayed externally. Message is trained as legitimate mail or spam as determined by Intercept Anti-Spam if **Train** is also selected.

> **Note** *The Relay or Trust action can only be used with an Envelope message part because attempted relays must be rejected immediately after the envelope transaction.*

- **Accept** – Mail is accepted and is delivered regardless if the message is considered spam. Message is trained as legitimate mail if **Train** is also selected.
- **Certainly Spam** – Mail is received, trained as spam, and then the Intercept action for Certainly Spam is applied.
- **Just Log** – Take no action, but log the occurrence. Just Log can be used to override other lower priority Pattern Filters to test the effect of Pattern Filters without an action taking place.
- **SecureMail Encrypt** – Encrypts the message with the integrated SecureMail encryption engine.

> **Note** *If SecureMail Email Encryption is disabled globally, messages are delivered unencrypted when triggered by a Pattern Filter.*

- **PostX Encrypt** – Encrypts the message with the integrated PostX encryption engine.
- **BCC** – Send a blind carbon copy mail to the mail address specified in **Action Data** text box. This option only appears if you have a BCC email address set up in the Custom Actions page.
- **Do Not Train** – Do not use the message for Token Analysis training.

These actions appear in this list if they are defined in the Custom Actions page:

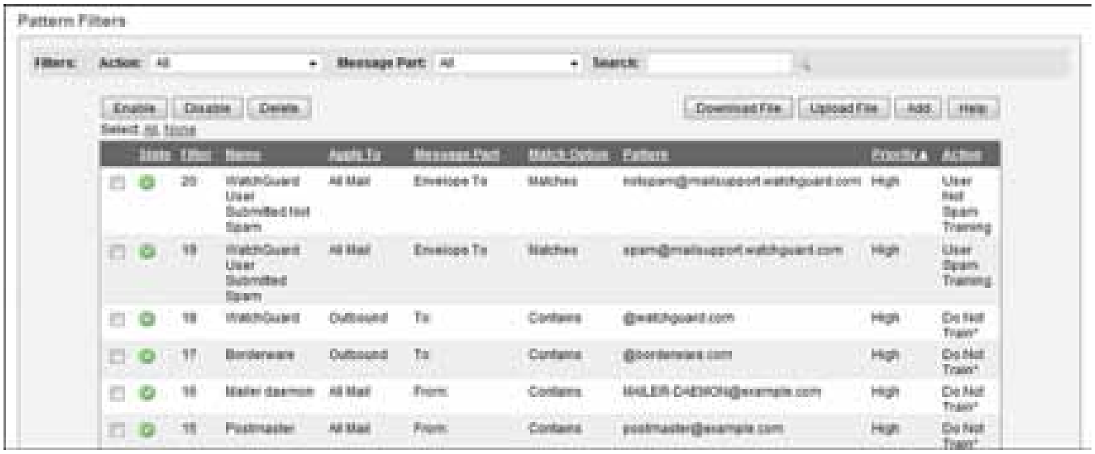
- **Discard** – Discards the message and does not send a notification to the sending server.
- **Quarantine** – Place the message into the administrative quarantine area.
- **Redirect to** – Redirects the message to the mail address or server specified in the **Action Data** field.
- **Encrypt** – Redirects the message to an encryption server.
- **Decrypt** – Redirects the message to a decryption server.
- **Archive (High, Medium, Low)** – Redirects the message to an archiving server.

11. In the **Comment** text box, enter a description for the Pattern Filter so that you can easily identify its purpose.
    The comment can only consist of letters, numbers, spaces, periods, underscores, and dashes.
12. Click **Apply**.

Search and Sort Pattern Filters

Use the search controls at the top of the Pattern Filters page to filter the list. You can select a specific action from the **Action** drop-down list, or a message part from the **Message Part** drop-down list.

To search by keyword, type specific search text in the **Search** text box.



Pattern Filters

Filters: Action: All Message Part: All Search:

	State	Filter	Name	Apply To	Message Part	Match Option	Pattern	Priority ▲	Action
□	●	20	WatchGuard User Submitted Not Spam	All Mail	Envelope To	Matches	notspam@mailsupport.watchguard.com	High	User Not Spam Training
□	●	19	WatchGuard User Submitted Spam	All Mail	Envelope To	Matches	spam@mailsupport.watchguard.com	High	User Spam Training
□	●	18	WatchGuard	Outbound	To	Contains	@watchguard.com	High	Do Not Train*
□	●	17	Borderware	Outbound	To	Contains	@borderware.com	High	Do Not Train*
□	●	16	Mailer daemon	All Mail	From	Contains	MAILER-DAEMON@example.com	High	Do Not Train*
□	●	15	Postmaster	All Mail	From	Contains	postmaster@example.com	High	Do Not Train*

To sort the list of Pattern Filters, click on a specific column title. For example, to sort the list by priority, click the **Priority** column.

Upload and Download Pattern Filters

You can create a list of Pattern Filters and upload them in a text file. The file must contain comma or tab separated entries.

Use this format:

```
[section],[type],[pattern],[action],[sequence(priority)],[rulenumber],[direction
(inbound, outbound, both],[options (on or ‘blank’)],[name],[is_enabled (t or
f)],[comments]
```

For example:

```
to:,contains,friend@example.com,reject,medium,1,both,on,patternname,t,comment
```

The **Options** field is used for the **Do-Not-Train** option. The value can be **on** or blank. If the field is blank, a **Reject** action is considered **Reject+Train**.

You must use a text editor to create the file pbmf.csv.

To update a Pattern Filter file:

1. To download the Pattern Filter list from the WatchGuard XCS, click **Download File**.
2. Open the file and update the Pattern Filter list.
3. Click **Upload File** and upload the edited file to the WatchGuard XCS.

Content Rules

Content rules allow you to create customized rule conditions for examining email message content and perform customized actions based on the search criteria.

> ***Note*** *Content Rules cannot be used with HTTP Web requests.*

A rule can contain one or several conditions, and the specified action is performed on the message if the conditions in the rule are satisfied. Rules can be ordered in priority as required. You can enable Content Rules globally, and you can also configure rules in the **Content Control** section of a policy.

> ***Note*** *You must enable the Pattern Filters feature for Content Rules to work properly. Content Rules are processed after Pattern Filters. To prevent issues with rule order processing, we recommend that you use either one method or the other when creating rule filters, and do not use both concurrently.*

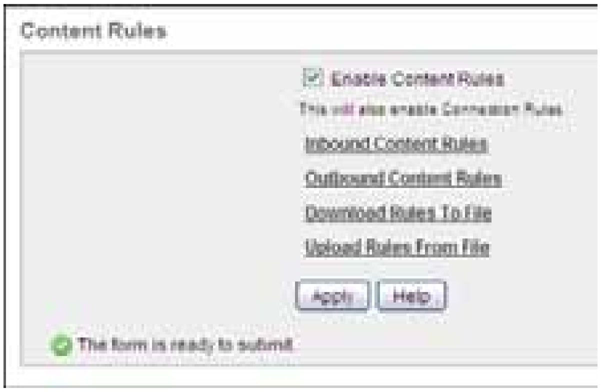
When you use Content Rules in conjunction with Trusted/Blocked Senders Lists, note this behavior:

- Users listed in the Trusted Senders List override any Content Rule action except if the rule action is Quarantine, Reject, or Discard.
- Users listed in the Blocked Senders List override a Content Rule action unless the Content Rule action is Reject or Discard.

Configure Content Rules

To configure and create Content Rules:

1. Select **Security > Content Control > Pattern Filters** and make sure you enable Pattern Filters.
2. Select **Security > Content Control > Content Rules**.
   The Content Rules page appears.



Content Rules

☑ Enable Content Rules

This will also enable Connection Rules

Inbound Content Rules

Outbound Content Rules

Download Rules To File

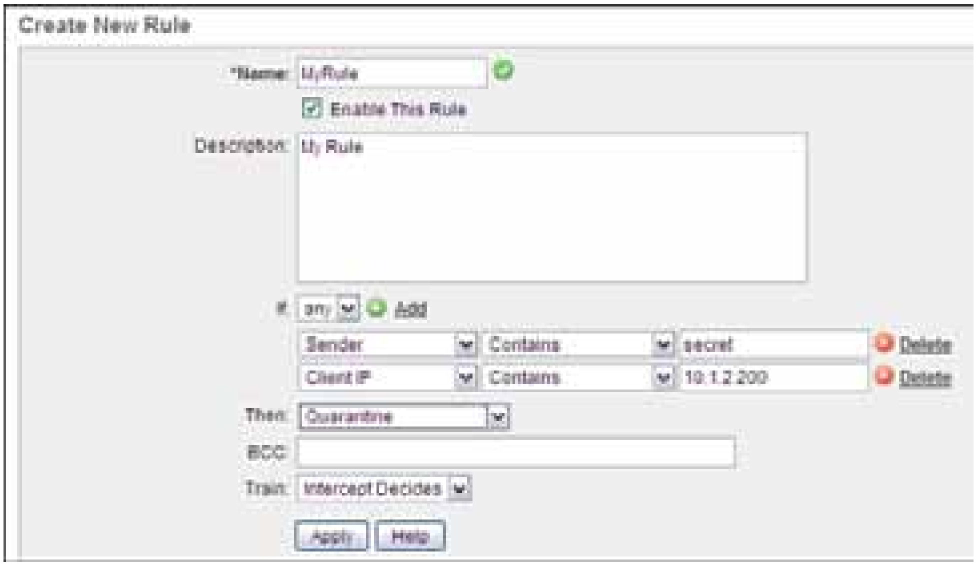
Upload Rules From File

The form is ready to submit.

3. Select the **Enable Content Rules** check box.

   Enabling Content Rules also enables Connection Rules that are configured in **Security > Anti-Spam > Connection Control**.

4. Select **Inbound Content Rules** to create rules for inbound traffic.
5. Select **Outbound Content Rules** to create rules for outbound traffic.
6. Click **Create New Rule**, or select an existing rule to modify its settings.



Create New Rule

*Name: MyRule

☑ Enable This Rule

Description: My Rule

If: any Add

Sender	Contains	secret	Delete
Client IP	Contains	10.1.2.200	Delete

Then: Quarantine

BCC:

Train: Intercept Decides

7. In the **Name** text box, type a name for this content rule.
8. Select the **Enable This Rule** check box.
9. In the **Description** text box, type a detailed description for the rule.
10. From the **If** drop-down list, select **all** if all conditions in this content rule must be true to trigger an action, or select **any** to trigger an action if any condition in the content rule is true.
    To add multiple conditions, click the "+" icon. To delete conditions, click the "x" icon. You can only have a maximum of 10 conditions per rule.
11. From the drop-down list, select a **Message Part** for this rule condition.
    - **Trusted** – The rule only acts on messages that are considered trusted by the system.
    - **Untrusted** – The rule only acts on messages that are considered untrusted by the system.

- **Mail Envelope** – This parameter allows for a match in any part of the message envelope which includes the HELO, Client IP, and Client Host.
- **HELO** – This parameter allows for a match in the HELO part of the message envelope. For example, mail.example.com.
- **Client IP** – This parameter allows for a match in the IP address of the system initiating the SMTP connection. For example, 10.1.2.200.
- **Client Host** – This parameter allows for a match in the client host name of the system initiating the SMTP connection. For example, mail.example.com.
- **Envelope Addr** – This parameter allows for a match in the Envelope To or Envelope From. For example, fred@example.com.
- **Envelope To** – This parameter allows for a match in the Envelope To field. For example, user@example.com.
- **Envelope From** – This parameter allows for a match in the Envelope From field. For example, user@example.com.
- **Mail Header** – This parameter allows for a match in any part of the message header.
- **Recipient** – This parameter allows for a match in the To: or Cc: fields.
- **Cc** – This parameter allows for a match in the Cc: field.
- **From** – This parameter allows for a match in the From: field.
- **Message-ID** – This parameter allows for a match in the Message-ID: field.
- **Received** – This parameter allows for a match in the Received: field.
- **Reply-to** – This parameter allows for a match in the Reply-to: field.
- **Sender** – This parameter allows for a match in the Sender: field.
- **Subject** – This parameter allows for a match in the Subject: field.
- **To** – This parameter allows for a match in the To: field.
- **Raw Mail Body** – This parameter allows for a match in any part of the encoded message body. This encoded content includes Base64, MIME, and HTML. Because messages are not decoded, a simple text match may not work. Use Mail Content for text matching on the decoded content.
- **Mail Content** – This parameter allows for a match on the visible decoded message body.
- **STA (Token Analysis) Token** – You can select Token Analysis tokens for a rule. This allows you to match patterns for common spam words that can be hidden or disguised with fake or invisible HTML text comments, which would not be caught by a normal content rule. For example, Token Analysis is able to extract the token “viagra” from the text “vi<spam>ag<spam>ra” and “v.i.a.g.r.a.”.
- **Content Scanning** – Matches the content of an entire message and its attachments. This field is used with the Content Scanning feature.
- **DFP Scanned** – The rule only acts on messages that have been scanned by Document Fingerprinting.
- **DFP Metric** – This parameter allows for a match in the Document Fingerprinting metric score, for example, equal to, greater than, and less than.

12. In the drop-down list, select the **Match Option** for the search:

- **Contains** – Looks for the text contained in a line or field. This allows for spaces or other characters that can make an exact match fail.
- **Starts with** – Looks for the text at the start of the line or field (no characters between the text and the start of line.)
- **Ends with** – Looks for the text at the end of the line or field. No characters, spaces are allowed between the text and the non-printed end-of-line character.
- **Matches** – The entire line or field must match the text exactly as entered.

- **Raw Regex** – Allows you to enter a regular expression for your search criteria.
- **In Dictionary** – Select a predefined dictionary that is matched against the specified message part.

13. In the search text box, type the specific text to search for.
14. From the **Then** drop-down list, select an action to perform when the rule statement is true:

> ***Note*** *You can define custom actions for use with Content Rules. See Custom Actions for Pattern Filters and Content Rules for details.*

- **Continue** – No action is taken and the message continues to be processed by the system. This is the default selection if no action is specified. BCC actions are still performed.
- **Quarantine** – Place the message into the administrative quarantine area.
- **Just log** – Log the event and take no further action.
- **Reject** – Reject the message and send a notification to the sending system.
- **Discard** – Discard the message and do not send a notification to the sending system.
- **Modify Subject Header** – Insert the specified text into the message subject line.
- **Add Header** – The specified “X-” mail header is added to the message headers.
- **Redirect To** – The message is delivered to the specified mail address or server.
- **Accept** – Mail is accepted and is delivered regardless if the message is considered spam.
- **SecureMail encrypt** – Encrypts the message with the integrated SecureMail encryption engine.
- **PostX encrypt** – Encrypts the message with the integrated PostX encryption engine.
- **PBMF Action** – Use a custom pattern filter action as defined in the Pattern Filter configuration.
- **Encrypt** – Redirects the message to the encryption server specified in the **Configuration > Mail > Encryption > External Encryption** menu.
- **Decrypt** – Redirects the message to the decryption server specified in the **Configuration > Mail > Encryption > External Encryption** menu.
- **Archive** – Redirects the message to an archive server specified in the **Configuration > Mail > Archiving** menu. Archive priority can be set to **Low**, **Medium**, and **High**.

15. In the **BCC** text box, type an optional email address to send a blind carbon copy of the message to if the rule is matched.
16. From the **Train** drop-down list, select the training options for this rule if it is matched.

- **Intercept decides** – The Intercept Anti-Spam engine decides whether to train the message as spam or legitimate mail based on its scanning results.
- **Do not train** – The message is not be trained.
- **Train as ham** – The message is trained as a legitimate (ham) message.
- **Train as spam** – The message is trained as a spam message.

17. Click **Apply**.

Rule Ordering

The rules are processed in the displayed order. To reorder rules, select a specific rule and drag it to the desired location. Click **Save Rule Order** to save the updated order of your rules when you are finished.

Download and Upload Content Rules

You can create a list of Content Rules and upload them in a text file. The file must contain comma or tab separated entries.

Use this format:

```
[Policy],[Stage],[Rank],[Name],[Description],[Enabled],[Condition],[Final
Action],[Final Action Text],[BCC Address],[Train Action]
```

For example:

```
0,1,50,Rule_10,This_is_Rule_10,1,pbmf_match(sender:,contains,”spammer”),subject_
rewrite,[Spam],admin@example.com,do_not_train
```

You must use a text editor to create the file contentrules.csv.

To update a Content Rules file:

1. To download the Content Rules list from the WatchGuard XCS, click **Download File**.
2. Open the file and update the Content Rules list.
3. Click **Upload File** and upload the edited file to the WatchGuard XCS.

This table describes the fields for the rules file:

Field	Description
Policy	Policy ID of the rule. This is 0 for a connection rule.
Stage	This is 1 if the rule is an inbound content rule, 2 if the rule is an outbound content rule, and 0 if a connection rule.
Rank	The ordering of the rule in the given policy and stage. 1 is the highest priority, 2 is next highest priority, and so on.
Name	The rule name.
Description	Description of the rule.
Enabled	This value is 1 if the rule is enabled, and 0 if it is disabled.
Condition	Rule condition statement: - trusted - !trusted (not trusted) - in_dict(messagepart,dictionaryID). For example, in_dict(client_hostname,83) - pbmf_match(messagepart, ptype, text). For example, pbmf_match(sender:,contains,”spammer”) in the previous example. *messagepart*: “env”, “helo”, “ip”, “client”, “env-addr”, “env-to”, “env-from”, “body”, “content”, “token”, “acs”, “hdr”, “recipient”, “cc:”, “from:”, “received:”, “reply-to:”, “sender:”, “subject:”, “to:”, “message-id”. *ptype* values: “contains”, “ends”, “starts”, “match”, “regex”. *text*: The specified text string. Boolean operators for “all” and “any” options: && - and, used with the “all” option

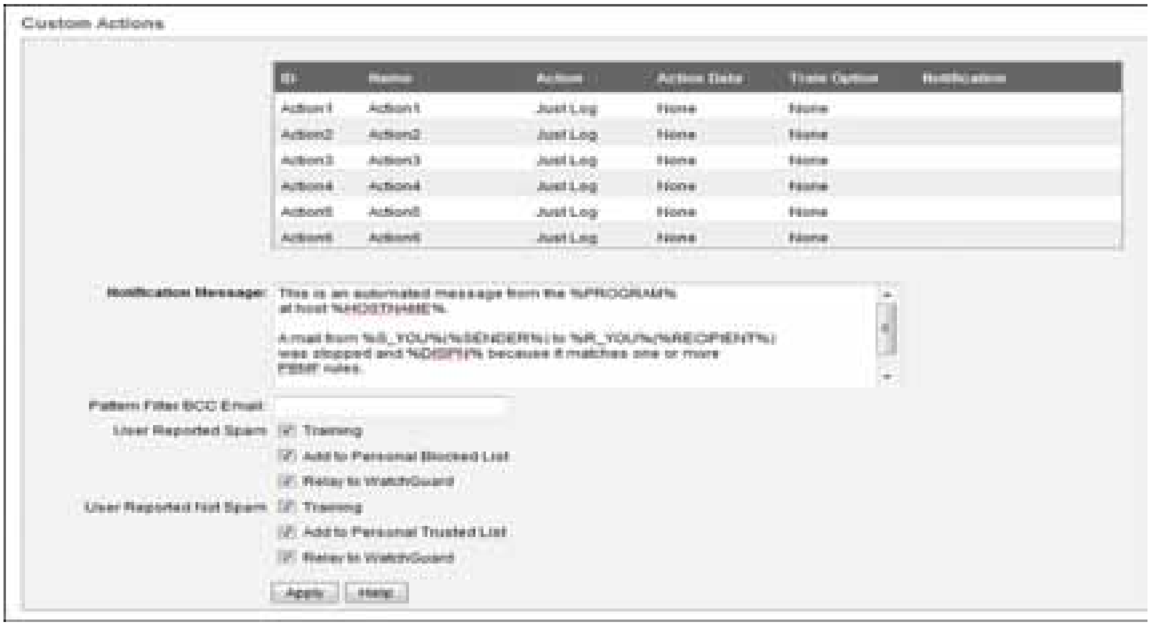
Field	Description
	|| - or, used with the “any” option For example, trusted&&in_dict(sender_address,83)&&pbmf_match(subject:,contains,”spam”)
Final action	Indicates the final rule action. This includes: “movem” (Quarantine), “log”, “trash” (Discard), “reject”, “subject_rewrite”, “add_header”, “redirect”, "sm_encrypt" (Encrypt), “postxenc” (Encrypt), “trust”, “relay”, “whitelist” (Accept), “continue”. Custom Pattern Filter actions. This includes external Encryption and Archiving if enabled: “actiona”, “actionb”, “actionc”, “actiond”, “actione”, “action1”, “action2”, “action3”, “action4”, “action5”, and “action6”.
Final action data	Indicates any additional data for the action, for example, the text for a modified subject or header, for example, “[Spam]” in the previous example.
BCC address	Contains a blind carbon email address, for example, user@example.com. This is blank if no address is specified.
Train action	This field is blank if set to the default “Intercept decides”. Other values include: “do_not_train”, “train_spam”, and “train_ham”.

Custom Actions for Pattern Filters and Content Rules

You can create additional custom actions that you can use with Pattern Filters and Content Rules. For example, you can only use the **Quarantine**, **Discard**, and **Redirect** actions for a Pattern Filter when defined as a custom action.

To create custom Pattern Filter or Content Rule actions and notifications:

1. Click **Security > Content Control > Custom Actions**.



Custom Actions

ID	Name	Action	Action Data	Train Option	Notification
Action1	Action1	Just Log	None	None	
Action2	Action2	Just Log	None	None	
Action3	Action3	Just Log	None	None	
Action4	Action4	Just Log	None	None	
Action5	Action5	Just Log	None	None	
Action6	Action6	Just Log	None	None	

Notification Message: This is an automated message from the %PROGRAM%
at host %HOSTNAME%.

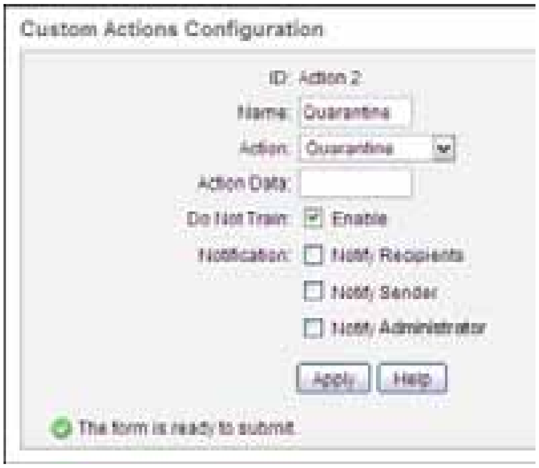
A mail from %S_YOU%(%SENDER%) to %R_YOU%(%RECIPIENT%)
was stopped and %DISP% because it matches one or more
PBMF rules.

Pattern Filter BCC Email:

User Reported Spam: ☑ Training
☑ Add to Personal Blocked List
☑ Relay to WatchGuard

User Reported Not Spam: ☑ Training
☑ Add to Personal Trusted List
☑ Relay to WatchGuard

2. Click on a specific custom action to define its options.
   You can define up to six custom actions.



Custom Actions Configuration

ID: Action 2

Name: Quarantine

Action: Quarantine

Action Data:

Do Not Train: ☑ Enable

Notification: ☐ Notify Recipients
☐ Notify Sender
☐ Notify Administrator

The form is ready to submit.

3. In the **Name** text box, type a description for the action.
4. From the **Action** drop-down list, select a custom action to perform:

   - **Reject** – Rejects the message and sends a notification to the sending server.
   - **Discard** – Discards the message and does not send a notification to the sending server.
   - **Quarantine** – Place the message into the administrative quarantine area.
   - **Certainly Spam** – Mail is received, trained as spam, and then the Intercept action for Certainly Spam is applied.
   - **Redirect to** – Redirects the message to the mail address or server specified in the **Action Data** field.
   - **Accept** – Accepts and delivers the message.
   - **BCC** – The message is copied to the email address specified in the **Action Data** field.

5. In the **Action Data** text box, type the action data for the specified **Action**.

   For the **Redirect To** action, send the message to a mailbox, for example, spam@example.com. You can also specify a domain, for example, spam.example.com. For a **BCC** action, type an email address to which to send a blind carbon copy of the message.

6. Select the **Do Not Train** option to make sure that when this action is performed, the message is not trained for spam.
7. In the **Notification** section, select the users that receive a notification when the custom action is applied.

   - **Notify Sender** – Sends a notification to the sender of the message.
   - **Notify Recipient** – Sends a notification to the recipients of the message.
   - **Notify Administrator** – Sends a notification to the WatchGuard XCS administrator.

8. Click **Apply**.
9. In the **Notification Message** text box, type a custom notification message for the action.
10. In the **PBMF BCC Email Address** text box, type an email address to use in conjunction with the **BCC** action to specify the email address to which to send a blind carbon copy message.
11. Click **Apply**.

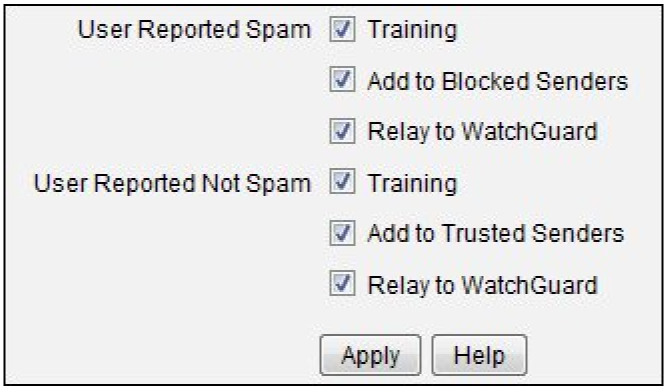
User Reported Spam and Not Spam

End users can utilize a Microsoft Outlook Add-in from WatchGuard that places special **Spam** and **Not Spam** buttons on their Outlook client toolbar. This tool allows the user to report any spam messages that bypassed the spam filters and were delivered to their inbox, and also report false positives where legitimate messages were classified as spam.

See *WatchGuard XCS Outlook Add-in* for more detailed information on installing and configuring the Outlook Add-in.

User Reported Spam

Select your options for spam reported from end users:



User Reported Spam ☑ Training
☑ Add to Blocked Senders
☑ Relay to WatchGuard
User Reported Not Spam ☑ Training
☑ Add to Trusted Senders
☑ Relay to WatchGuard

- **Training** – Enables training on user submitted spam messages.
- **Add to Blocked Senders** – When a user submits messages as spam, the sender is automatically added to their personal Blocked Senders List.

- **Relay to WatchGuard** – Allows user submitted spam messages to be relayed to WatchGuard servers for training. Disable this option to use training messages for your device only and not share them with WatchGuard.

User Reported Not Spam

Select your options for legitimate mail (Not Spam) reported from end users:

- **Training** – Enables training on user submitted legitimate (Not Spam) messages.
- **Add to Trusted Senders** – When a user submits messages as legitimate mail (Not Spam), the sender is automatically added to their personal Trusted Senders List.
- **Relay to WatchGuard** – Allows user submitted legitimate messages (Not Spam) to be relayed to WatchGuard servers for training. Disable this option to use training messages for your device only and not share them with WatchGuard.

> ***Warning*** *If you import Trusted/Blocked Senders Lists from a WatchGuard QMS (Quarantine Management Server), the import will overwrite any entries created by user submitted spam and legitimate mail from the WatchGuard XCS Outlook Add-in.*

Reroute Mail with Pattern Filters

You can use custom Pattern Filters to redirect mail to another mail server, while preserving the message properties (for example, Envelope To and Deliver To). This feature is similar to the redirect actions and reroute mail routes used in Archiving and External Encryption to redirect mail to an archiving or encryption server.

In your mail routing configuration (configured in **Configuration > Mail > Routing**), create a mail route that begins with a "." period character, (for example, `.mail_reroute`) and enter the destination mail server as the address for your mail route.

When you create a custom Pattern Filter, set the **Action** to **Redirect To**, and in the **Action Data** field, type the name of the corresponding mail route, for example, `mail_reroute`.

When a pattern filter is matched, it reroutes the message to the corresponding mail server.

Connection Rules

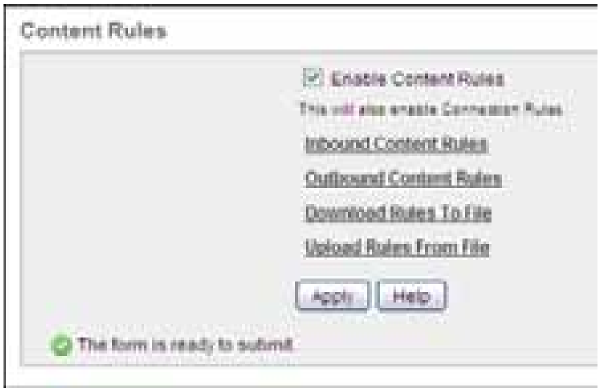
Connection Rules allow the administrator to create customized rule conditions for examining incoming and outgoing message connections, to perform customized actions based on the search criteria. A rule can contain one or several conditions. The specified action is performed on the message if the conditions in the rule are satisfied. Rules can be ordered in priority as required.

> ***Note*** *Connection Rules are processed after Specific Access Patterns and Pattern Filters. To prevent issues with rule order processing, do not use both methods concurrently.*

To configure Connection Rules:

1. To enable Connection Rules, you must first enable the Content Rules feature in **Security > Content Control > Content Rules**.

2. Select the **Enable Content Rules** check box.
3. Click **Apply**.



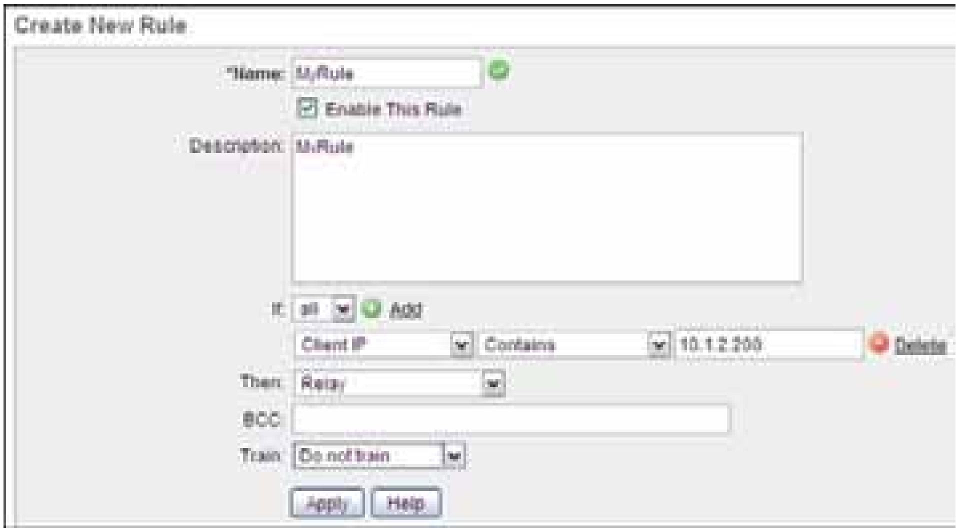
Content Rules

☑ Enable Content Rules

This will also enable Connection Rules

The form is ready to submit.

4. Select **Security > Anti-Spam > Connection Control**.
5. Select **Connection Rules**.
6. Click **Create New Rule**, or select an existing rule to modify its settings.



Create New Rule

*Name: MyRule

☑ Enable This Rule

Description: MyRule

If: all

Client IP | Contains | 10.1.2.200

Then: Relay

BCC:

Train: Do not train

7. In the **Name** text box, type a descriptive name for this rule.
8. Select the **Enable This Rule** check box.
9. In the **Description** text box, type a detailed description for the rule.
10. From the **If** drop-down list, select **all** if all conditions in this content rule must be true to trigger an action, or select **any** to trigger an action if any condition in the content rule is true.
    To add multiple conditions, click the "+" icon. To delete conditions, click the "x" icon. You can only have a maximum of 10 conditions per rule.
11. From the drop-down list, select a **Message Part** for this rule condition.
    - **Trusted** – The rule acts only on messages that are considered trusted by the system.
    - **Untrusted** – The rule acts only on messages that are considered untrusted by the system.
    - **Mail Envelope** – This parameter allows for a match on any part of the message envelope which includes the HELO, Client IP, and Client Host.
    - **HELO** – This parameter allows for a match on the HELO part of the message envelope. For example, mail.example.com.

- **Client IP** – This parameter allows for a match on the IP address of the system initiating the SMTP connection. For example, 10.1.2.200.
- **Client Host** – This parameter allows for a match on the client host name of the system initiating the SMTP connection. For example, mail.example.com.
- **Envelope Addr** – This parameter allows for a match on the Envelope To or Envelope From. For example, fred@example.com.
- **Envelope To** – This parameter allows for a match on the Envelope To field. For example, fred@example.com.
- **Envelope From** – This parameter allows for a match on the Envelope From field. For example, fred@example.com.

12. In the drop-down list, select the **Match Option** for the search:
    - **Contains** – Looks for the text contained in a line or field. This allows for spaces or other characters that may make an exact match fail.
    - **Starts with** – Looks for the text at the start of the line or field (no characters between the text and the start of line.)
    - **Ends with** – Looks for the text at the end of the line or field. No characters, spaces, are allowed between the text and the non-printed, end-of-line character.
    - **Matches** – The entire line or field must match the text exactly as entered.
    - **Raw Regex** – Allows you to enter a regular expression for your search criteria.
    - **In Dictionary** – Select a predefined dictionary that is matched against the specified message part.
13. In the search text box, type the specific text to search for.
14. From the **Then** drop-down list, select an action to perform when the rule statement is true:
    - **Continue** – No action is taken and the message continues to be processed by the system. This is the default selection if no action is specified. BCC actions are still performed.
    - **Quarantine** – Place the message into the administrative quarantine area.
    - **Just log** – Log the event and take no further action.
    - **Reject** – Reject the message and send a notification to the sending system.
    - **Discard** – Discard the message and do not send a notification to the sending system.
    - **Modify Subject Header** – Insert the specified text into the message subject line.
    - **Add Header** – Add the specified "X-" mail header to the message headers.
    - **Redirect To** – The message is delivered to the specified mail address or server.
    - **Accept** – Mail is accepted and is delivered regardless if the message is considered spam.
    - **PostX encrypt** – Encrypts the message with the integrated PostX encryption engine.
    - **SecureMail encrypt** – Encrypts the message with the integrated SecureMail encryption engine.
    - **Trust** – This mail is considered trusted and from a legitimate source. This message is not processed for spam.
    - **Relay** – Allows the message to be relayed externally.
    - **PBMF Action** – Use a custom pattern filter action, as defined in the Pattern Filter configuration.
    - **Encrypt** – Redirects the message to an encryption server.
    - **Decrypt** – Redirects the message to a decryption server.
15. In the **BCC** text box, type an optional email address to send a blind carbon copy of the message to if the rule is matched.
16. From the **Train** drop-down list, select the training options for this rule if it is matched.
    - **Intercept decides** – The Intercept Anti-Spam engine decides whether to train the message as spam or legitimate mail based on its scanning results.
    - **Do not train** – The message is not be trained.

- **Train as ham** – The message is trained as a legitimate (ham) message.
- **Train as spam** – The message is trained as a spam message.

17. Click **Apply**.

Rule Ordering

The rules are processed in the displayed order. To reorder rules, select a specific rule and drag it to its desired location. Click **Save Rule Order** to save the updated order of your rules when you are finished.

Dictionaries and Lists

The Dictionaries and Lists feature contains default and custom word and phrase dictionaries that you can use with the Objectionable Content Filter, Spam Dictionaries, and Content Scanning features. You can also create lists of IP addresses, domains, and email addresses to use with the Blocked and Trusted web sites feature.

Each dictionary or list is a simple word or phrase text file (in Unix format) with one word or phrase per line:

```
ComplianceClassified
Top Secret
This is Confidential
```

The maximum word length is 35 characters. You can upload words or phrases greater than 35 characters, but they are truncated for matching purposes. Both plural and singular word forms must be defined in the dictionaries. In policies, the phrase length of the compliance dictionary selected should not be greater than the phrase length configured in the content scanning configuration.

Character Set Support

The WatchGuard XCS supports several characters sets for dictionary-based message scanning. This allows you to upload dictionaries in a variety of language character set encodings and use these dictionaries with the Objectionable Content Filter when scanning email and web content.

> **Note** *Non-English character sets cannot be used with the Content Scanning feature.*

These character set encodings are supported for use in dictionaries:

- ASCII
- Unicode
- UTF-8, UTF-16, UTF-32
- ISO-8859-1 (Western European Languages)

> **Note** *Only languages that can be converted to ISO-8859-1 and Big Endian byte order character set encodings are supported.*

When a dictionary is uploaded, the system converts the file’s contents to ISO-8859-1 for use with the internal scanners. The file is displayed in ISO-8859-1 format on the Dictionaries page. Downloading the dictionary saves it in the original character encoding format with which it was uploaded.

Only languages that can be converted to ISO-8859-1 (Western European Latin-based Character Set) are supported.

For email messages, incoming data is assumed to be in the ISO-8859-1 character set. UTF-8, double byte, or multi-byte content are not processed properly. This content cannot be matched to a dictionary scanning-based feature and passes through the WatchGuard XCS without being blocked.

For web scanning, most web content is UTF-based. The WatchGuard XCS attempts to convert incoming data to the ISO-8859-1 character encoding for scanning. Any characters (primarily those that do not belong to the ISO-8859-1 character set) that cannot be converted into a single byte cannot be matched to a dictionary by the message scanners, and pass through without being blocked.

Your web browser must be configured to display the ISO-8859-1 character set to view the contents of the dictionary file. In addition, make sure the web server configuration (in **Configuration > Network > Web Server**), accurately reflects the encoding you require.

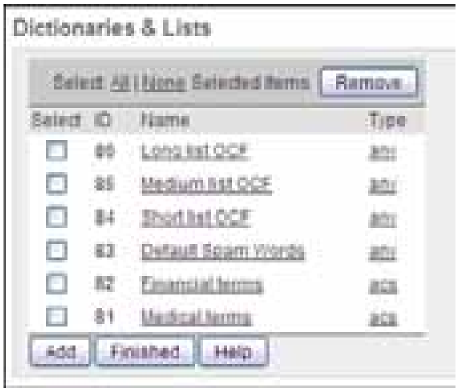
These languages are supported by the ISO-8859-1 character set:

- Afrikaans
- Albanian
- Basque
- Breton
- Danish
- Dutch (missing IJ, ij but these should always be represented as IJ or ij in electronic form)
- English (US and modern British)
- Estonian (missing Š, š, Ž, for loan words)
- Faroese
- Finnish (missing Š, š, Ž, for loan words)
- French (missing Œ, œ and the very rare Ÿ; they are generally replaced by "OE" and "oe" without the normally required ligature, and "Y" without the diaeresis)
- Galician
- German
- Icelandic
- Irish (new orthography)
- Italian
- Latin (basic classical orthography)
- Luxembourgish (basic classical orthography)
- Norwegian (Bokmål and Nynorsk)
- Occitan
- Portuguese (European and Brazilian)
- Rhaeto-Romanic
- Scottish Gaelic
- Spanish
- Swahili
- Swedish
- Walloon
- Welsh (missing these circumflex accented characters W, w, Y, y)

Add a Dictionary

To add a new dictionary to the system:

1. Select **Security > Content Control > Dictionaries & Lists**.

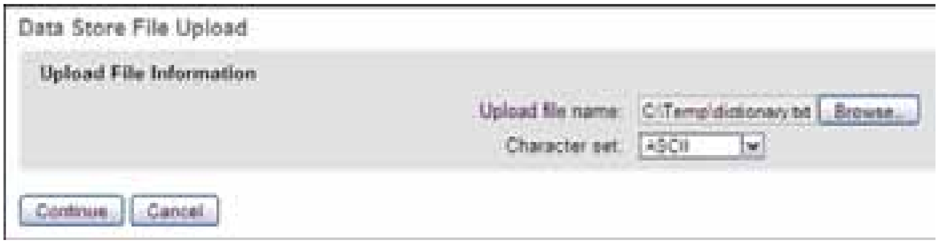


Dictionaries & Lists

Select All | None Selected Items Remove

Select	ID	Name	Type
□	86	Long list OCF	any
□	85	Medium list OCF	any
□	84	Short list OCF	any
□	83	Default Spam Words	any
□	82	Financial terms	acs
□	81	Medical terms	acs

2. Click **Add**.



Data Store File Upload

Upload File Information

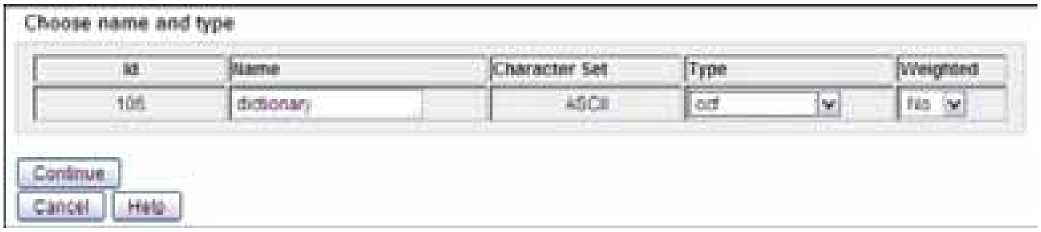
Upload file name: C:\Temp\dictionary.txt

Character set: ASCII

3. Click **Browse** to select a file to upload.
4. From the **Character set** drop-down list, select the encoding used in the uploaded file.

   The file must be in the character set encoding you specify. If it is not, unexpected results occur and the displayed dictionary file will not match its content (for example, accented characters not displayed properly). For example, if the file you upload is encoded with ISO 8859-1, you must select the
   ISO-8859-1 character set from the drop-down list. If the file is using UTF-8, you must select the UTF-8 character set from the drop-down list.

5. Click **Continue**.



Choose name and type

Id	Name	Character Set	Type	Weighted
106	dictionary	ASCII	ocf	No

6. In the **Name** text box, type a descriptive name for the dictionary or list.
7. From the **Type** drop-down list, select the type of file you are uploading:

   - **Any** – This file type can be used for any dictionary-based feature.
   - **ACS** – This file type of words and phrases is used with the policy-based content scanning feature.
   - **DFP** – This file type of words and phrases is used with the Document Fingerprinting feature.
   - **OCF** – This file type of objectionable words and phrases is used with Objectionable Content Filtering.

- **Spam** – This file type of spam words and phrases is used with the Spam Words Intercept Anti-Spam feature.
- **IP** – A list of IP addresses. For example, 192.168.1.128.
- **Email** – A list of email addresses. For example, user@example.com.
- **Domain** – A list of domains. For example, example.com.
- **CIDR** – A list of CIDR IP address networks. For example, 10.10.0.0/16.
- **Domain&email** – A list of domains and email addresses. For example, example.com,admin@example.com. These can be used for the Hosted Domains reporting feature.

8. Click **Continue** to finish uploading the file.
   The new dictionary appears in the list and can be selected when using a dictionary-based feature.

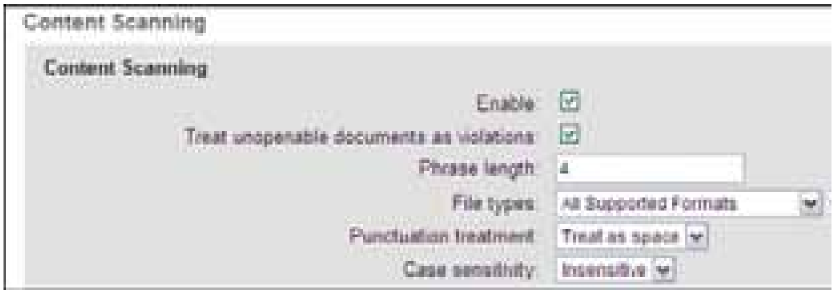
Financial and Medical Dictionaries

The WatchGuard XCS includes predefined dictionaries that contain industry-specific terms for medical and financial organizations to assist you with regulatory compliance configurations. You can customize these dictionaries to comply with specific regulations regarding the communications and storage of message data. The dictionaries are used with the Content Scanning feature to allow the system to check the dictionary for matched words and phrases in incoming and outgoing messages and attachments. You can use policies to define specific Content Scanning actions when dictionary terms are detected.

> ***Note*** *If you use the Financial and Medical dictionaries when content scanning email messages and web requests, you must review these dictionaries and customize them as appropriate for your organization to prevent legitimate messages from being blocked because of words and phrases in these dictionaries.*

To enable a dictionary for use in a Content Scanning policy:

1. Select **Security Policies > Content Control > Content Scanning**.
2. Select the **Enable** check box.



Content Scanning

Content Scanning

Enable ☑

Treat unopenable documents as violations ☑

Phrase length 4

File types All Supported Formats

Punctuation treatment Treat as space

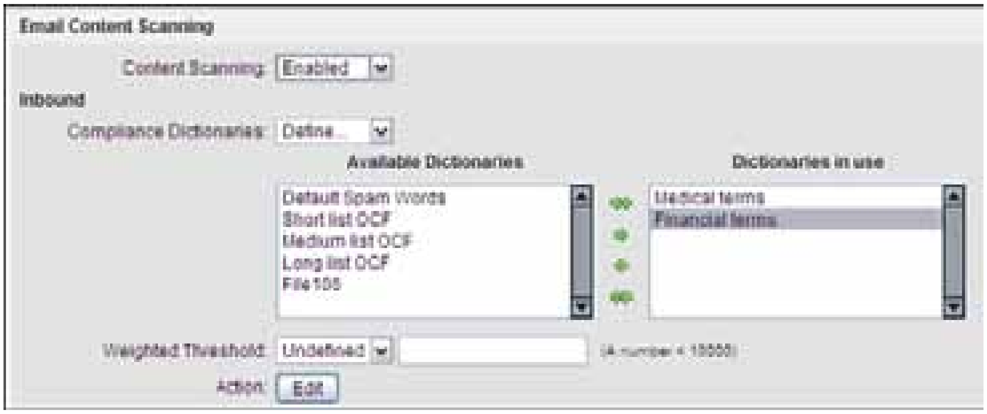
Case sensitivity Insensitive

3. In the **Phrase length** text box, type a phrase length for your specific dictionaries.

   The Content Scanning feature has a default Phrase length of 3, indicating that the system only scans up to 3 words of a dictionary phrase. If longer phrases appear in your Financial or Medical dictionaries, the Phrase length must be increased to 4 or more as required. Longer phrase lengths require additional system processing.

4. Click **Apply**.
5. Select **Policies**.
6. Select a policy to configure, for example, the **Default Policy** or another policy.

7. Select the **Edit** link in the **Content Control** section.
8. In the **Content Scanning** section, enable **Content Scanning** and select the required dictionary (for example, **Medical Terms**) from the **Compliance Dictionaries** drop-down list.



Email Content Scanning

Content Scanning: Enabled

Inbound

Compliance Dictionaries: Define...

Available Dictionaries: Default Spam Words, Short list OCF, Medium list OCF, Long list OCF, File105

Dictionaries in use: Medical terms, Financial terms

Weighted Threshold: Undefined (A number < 10000)

Action: Edit

9. From the **Action** field, click **Edit** to select the actions to perform for email messages and HTTP requests when a dictionary term is detected in a message or its attachments.

> **Note** *By default, the medical and financial dictionaries are configured with no weights. You can modify and customize the dictionaries as required with weights for each word or phrase.*

Weighted Dictionaries

You can assign a configurable weight to dictionary words and phrases to provide more intelligent and flexible decisions for dictionary scanner components and compliance policies.

With a weighted dictionary, you can perform an action if the aggregate weight of several matched dictionary terms exceeds a configurable threshold. You can set a weight to a dictionary word or phrase so that it is a compliance violation if any two terms from a dictionary appear in a message or attachment. The weight of these two terms is added together, and if they exceed the threshold for that policy, an action is performed.

For example, the WatchGuard XC S can encrypt an outbound message when the phrase “patient number” and the term “diagnosis” are detected in the same message content. In the weighted dictionary, these terms can be configured to have a weight of 50. If the weighted threshold for the compliance dictionary is set to 100, these two terms, or any number of terms that match or exceed a weight of 100, cause the message to be encrypted.

> **Note** *If the same word appears more than once in a message (this includes text and HTML portions of a message), each instance is included in the total weight.*

When a dictionary is configured as a weighted dictionary, use this format:

```
match,weight
```

or

```
weight,match
```

For example,

```
patient,30
```

or

```
50,diagnosis
```

The first line of the weighted dictionary must contain the heading **match,weight**, or **weight,match** depending on the configuration of your file.

For example,

```
match,weightpatient,30diagnosis,50
```

Negative Dictionary Weights

You can apply negative weights to specific words or phrases in a weighted dictionary that, on their own, may not constitute a match in an objectionable content or compliance dictionary. For example, a weighted dictionary entry can be entered as “junk,-25”. This indicates that if the word “junk” appears on its own in the text of a message, the weight threshold is lowered by 25. Another phrase entry can be entered as “junk message,50” that indicates that the phrase “junk message” raises the weight by 50. This helps to prevent weighted thresholds from being exceeded by words that may not be objectionable or classified for compliance, when they are not used in conjunction with other words or phrases.

When a dictionary is configured as a weighted dictionary, use this format:

```
match,weight
```

or

```
weight,match
```

For example,

```
patient,-30
```

or

```
50,diagnosis
```

The first line of the weighted dictionary must contain the heading **match,weight**, or **weight,match** depending on the configuration of your file.

For example,

```
match,weightpatient,-30diagnosis,50
```

Use Weighted Dictionaries

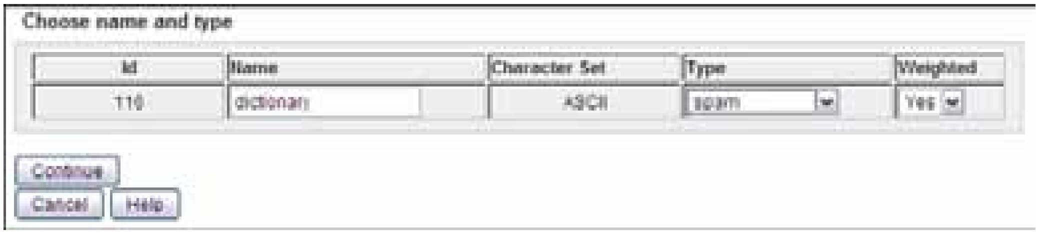
Weighted dictionaries can be used with Spam Words, Content Scanning, and the Objectionable Content Filter.

Create a dictionary with spam words and phrases and their assigned weights that are checked by the Spam Words scanning feature.

```
match,weightspam,40hot stocks,40viagra,50stock tips,40stock,-50
```

To upload a dictionary, select **Security > Content Control > Dictionaries & Lists**.

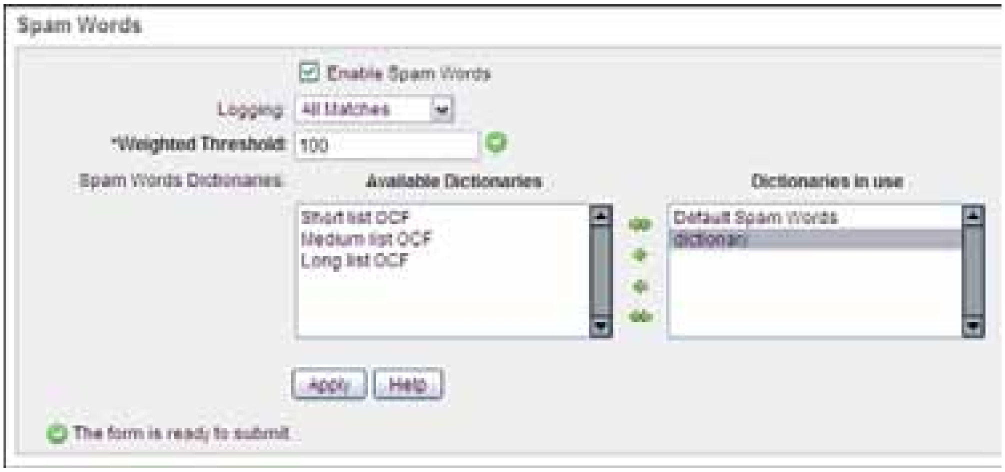
1. In the **Type** drop-down list, select **Spam** or **Any**.
2. From the **Weighted** drop-down list, select **Yes**.



Choose name and type

Id	Name	Character Set	Type	Weighted
116	dictionary	ASCII	spam	Yes

3. Select **Security > Anti-Spam > Anti-Spam > Spam Words**.
   The Spam Words page appears.



Spam Words

☑ Enable Spam Words

Logging: All Matches

*Weighted Threshold: 100

Spam Words Dictionaries:

Available Dictionaries	Dictionaries in use
Short list OCF	Default Spam Words
Medium list OCF	dictionary
Long list OCF	

The form is ready to submit.

4. Select **Enable Spam Words**.
5. In the **Weighted Threshold** text box, type the weighted threshold if you use weighted dictionaries with Spam Words

   This threshold can be any positive integer from 1 to 9999. In this example, the default threshold is 100. If the number of spam words in a message have an aggregate weight of 100 or more, the message is considered spam.

6. Select the weighted dictionary created in the first step.
7. Click **Apply**.

10 Intercept Anti-Spam

Intercept Anti-Spam Overview

The *Intercept Anti-Spam* features take advantage of the extensive message control features of the WatchGuard XCS to provide a solutions-based approach where each anti-spam component, when enabled, provides input to the final spam score of a message. Information retrieved by all of the enabled Anti-Spam components results in a more informed decision on whether a message is spam or legitimate mail.

You can set thresholds to take appropriate action on a message based on its score and classification, for example, *Certainly Spam*, *Probably Spam*, and *Maybe Spam*. You can set a different action for each threshold, for example, “Reject” for messages that are classified as *Certainly Spam*, or “Modify Subject Header” for messages that are classified as *Maybe Spam*.

WatchGuard has engineered the default Intercept configuration to provide maximum protection against spam without additional configuration, but you can modify the Intercept options to provide more granular control over each Anti-Spam Intercept component for your environment.

The Intercept Anti-Spam engine includes these components:

Spam Words

Filters messages based on a dictionary of typical spam words and phrases that are matched against the message.

Mail Anomalies

Checks various aspects of the incoming message for issues, for example, unauthorized SMTP pipelining, missing headers, and mismatched identification fields.

DNS Block List (DNSBL)

Detects spam using domain-based lists of hosts that have a poor reputation. Messages can also be rejected immediately, regardless of the results of other Anti-Spam processing, if the client is listed on a DNSBL. A configurable threshold allows you to specify how many DNSBLs must be triggered to consider the sender as unreliable.

URL Block List

URL Block Lists contain a list of domains and IP addresses of URLs that have appeared previously in spam messages. This feature examines any URLs contained in the body of a message to see if they appear on a block list.

Reputation Enabled Defense

The Reputation Enabled Defense service helps to identify spam by reporting behavioral information about the sender of a mail message, based on information collected from installed products and global DNS Block Lists. The statistics it collects include the sender's overall reputation, where the sender is a dial-up, and whether the sender appears to be virus-infected or sends large amounts of spam messages. The Intercept engine uses this information to reject the message, or uses it as part of the overall anti-spam decision. Reputation Whitelists allow you to train on messages from known legitimate sources based on their reputation.

Token Analysis

Detects spam based on advanced content analysis using databases of known spam and valid mail.

Backscatter Detection

Detects spam based on signature verification of the Envelope Sender to prevent spam bounce emails to forged sender addresses.

Sender Policy Framework (SPF)

Performs a check of a sending host’s SPF DNS records to identify and validate the source of a message to determine whether a message was spoofed.

DomainKeys Authentication

Performs a check of a sending host’s DomainKeys DNS records to identify and validate the source of a message to determine whether a message was spoofed.

Brightmail

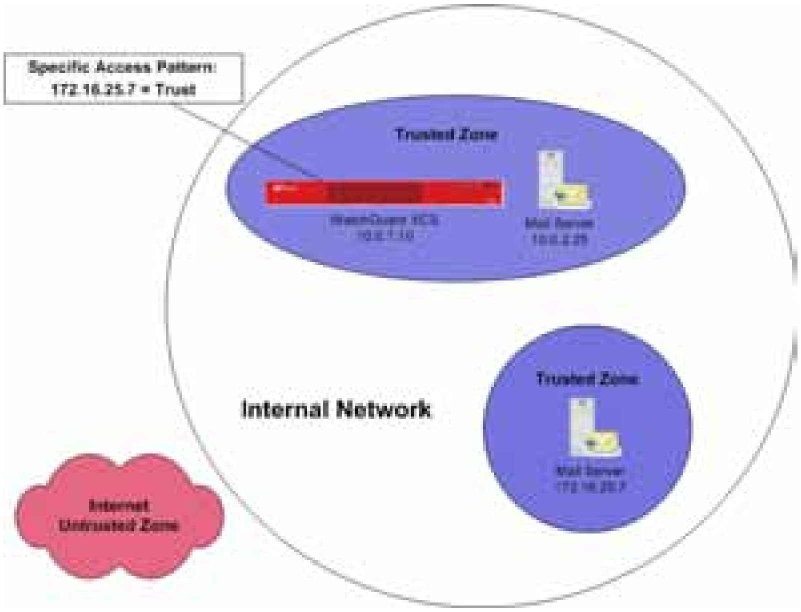
You can utilize the Symantec Brightmail Anti-Spam™ engine as a cost-option. Brightmail integrates into the overall Intercept spam score, or you can run Brightmail independently.

Trusted and Untrusted Mail Sources

You must configure the WatchGuard XCS to properly interact with local and remote mail servers. The XCS device only processes mail through the spam filters when a message originates from an untrusted source. Mail from trusted sources bypass the spam controls.

There are two ways to control how sources of mail are identified and trusted:

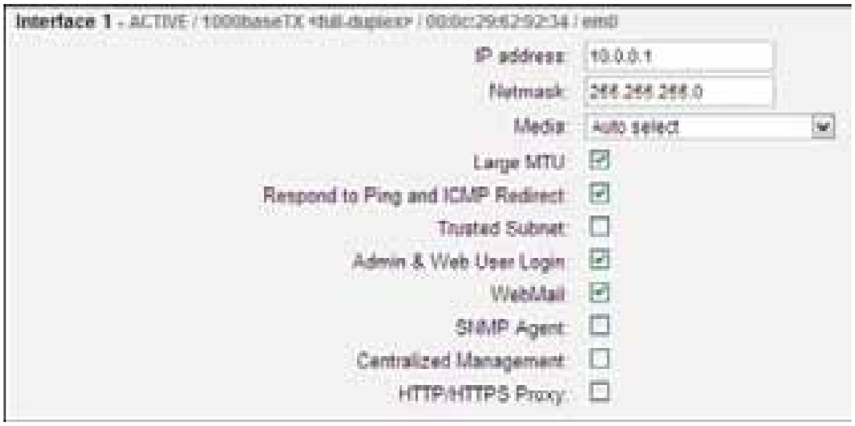
- **Trusted Subnet** – All mail from a specific network interface is considered trusted.
- **Specific Access Pattern** – An IP address (or address block), server, or domain name is identified as trusted by a specific access pattern rule.



Trusted Subnet

To specify a network interface as trusted or untrusted:

1. Select **Configuration > Network > Interfaces**.
2. Enable or disable the **Trusted Subnet** check box for the required interface.
   Do not enable the Trusted Subnet option if the device is deployed internally or behind a network firewall.



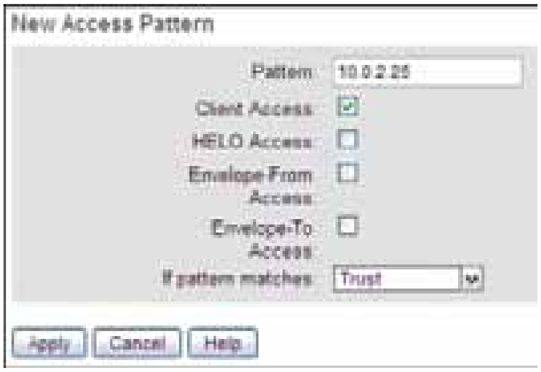
Interface 1 - ACTIVE / 1000baseTX <full-duplex> / 00:0c:29:62:92:34 / em0

IP address: 10.0.0.1
Netmask: 255.255.255.0
Media: Auto select
Large MTU: ☑
Respond to Ping and ICMP Redirect: ☑
Trusted Subnet: □
Admin & Web User Login: ☑
WebMail: ☑
SNMP Agent: □
Centralized Management: □
HTTP/HTTPS Proxy: □

Trust Servers with Specific Access Patterns

To trust a server with a Specific Access Pattern:

1. Select **Configuration > Mail > Access**.
2. In the **Specific Access Patterns** section, click **Add Pattern**.



New Access Pattern

Pattern: 10.0.2.25

Client Access: ☑

HELO Access: □

Envelope-From Access: □

Envelope-To Access: □

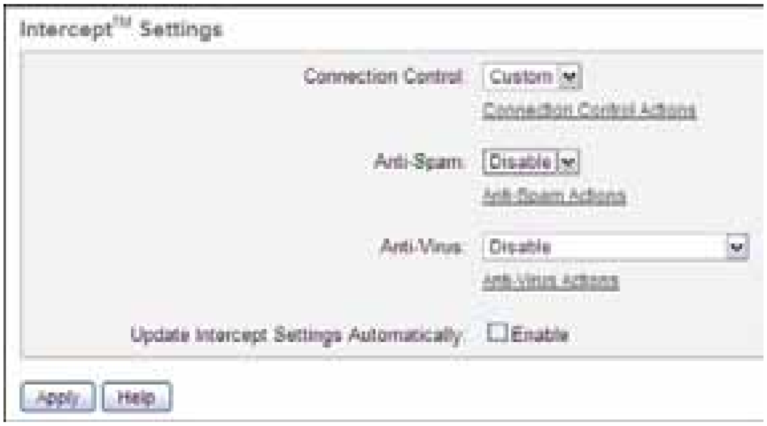
If pattern matches: Trust

3. In the **Pattern** text box, type the IP address or hostname of the server.
4. Select the **Client Access** check box.
5. From the **If pattern matches** drop-down list, select **Trust**.
6. Click **Apply**.

Intercept Settings

Select **Security > Anti-Spam > Intercept Settings** to configure global Intercept connection settings.

You can enable or disable Intercept's Connection Control, Anti-Spam, Anti-Virus features, and enable automatic update of advanced Intercept settings. If you change any default settings, the selection is listed as *Custom*.



Intercept™ Settings

Connection Control: Custom

Connection Control Actions

Anti-Spam: Disable

Anti-Spam Actions

Anti-Virus: Disable

Anti-Virus Actions

Update Intercept Settings Automatically: □ Enable

Intercept Connection Control

This table describes the default **Intercept Connection Control** settings when you enable Connection Control. To view the current actions and settings, click **Connection Control Actions**.

Feature	Default Setting
Reject on Reputation (Reputation Enabled Defense)	Enabled (Threshold: 90)
Reject on infection (Reputation Enabled Defense)	Enabled
Reject connections from dial-ups (Reputation Enabled Defense)	Off

Feature	Default Setting
Reject on DNSBL	Off
Threat Prevention	Enabled
Reject on unknown sender domain	Enabled
Reject on missing sender MX	Off
Reject on non FQDN sender	Enabled
Reject on unauth pipelining	Enabled
Reject on missing addresses	Off
Reject on missing reverse DNS	Off

Intercept Anti-Spam

This table describes the default **Intercept Anti-Spam** settings when you enable the Anti-Spam feature. To view the current actions and settings, click **Anti-Spam Actions**.

Intercept Option	Default Setting
Certainly Spam	Reject (Threshold: 99)
Probably Spam	Modify Subject Header (Threshold: 90)
Maybe Spam	Just Log (Threshold: 60)
Decision Strategy	Heuristic 1
Spam Words	Enabled
Mail Anomalies	Enabled
DNS/URL Block List	Enabled
Reputation Enabled Defense	Enabled
Token Analysis	Enabled
SPF	Enabled
DomainKeys	Enabled
Backscatter	Off

Intercept Anti-Virus

You can enable the Intercept Anti-Virus feature independently or with Outbreak Control. To view the current actions and settings, click the **Anti-Virus Actions** link.

Enable

Enables Anti-Virus scanning for both Inbound and Outbound directions. The action is set to **Quarantine Mail**. This action also enables Malformed Mail checks.

Enable with Outbreak Control

Enables Anti-Virus scanning for both Inbound and Outbound directions. The action is set to **Quarantine Mail**. This action also enables Outbreak control to quarantine possible virus-infected messages, and enables Malformed Mail checks.

Automatic Intercept Configuration

Select the **Update Intercept Settings Automatically** check box to allow advanced Intercept settings to be updated automatically by WatchGuard. If you use this option, WatchGuard will update your advanced Intercept settings on a periodic basis to make sure you always use the most up-to-date and recommended configuration. Your Intercept actions, thresholds, and component settings are not modified with this option.

> **Note** *Automatic Intercept configuration requires that Security Connection be enabled and running.*

This option configures these advanced settings:

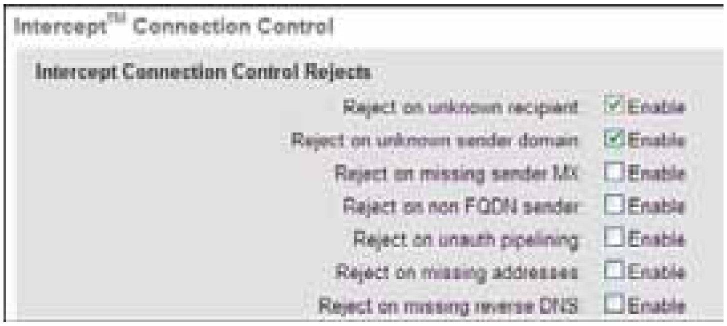
- Intercept Component Weights
- Reputation/UBL/DNSBL domains and timeout settings
- Advanced Token Analysis options
- Enable Image Analysis
- Enable PDF Analysis
- Analyze PDF text
- Analyze PDF images
- Enable RTF Analysis
- Legitimate mail and Spam training sources
- Legitimate mail and Spam limits and thresholds
- Dictionary spam count
- Reputation Whitelist

Intercept Connection Control

You can configure Intercept connection control settings to reject messages before the SMTP mail connection is completed based on several identifying factors about the connection.

To configure Connection Control settings:

1. Select **Security > Anti-Spam > Connection Control**.
   The Intercept Connection Control page appears.



Intercept™ Connection Control

Intercept Connection Control Rejects

Reject on unknown recipient ☑ Enable

Reject on unknown sender domain ☑ Enable

Reject on missing sender MX □ Enable

Reject on non FQDN sender □ Enable

Reject on unauth pipelining □ Enable

Reject on missing addresses □ Enable

Reject on missing reverse DNS □ Enable

Reject on unknown recipient

Rejects mail if the intended recipients do not exist locally or in an LDAP directory. See *Reject on Unknown Recipient* for more detailed information.

Reject on unknown sender domain

Rejects mail when the sender's mail address does not appear in the DNS as an A or MX record. This option only applies to untrusted mail.

Reject on missing sender MX

Rejects mail when the sender's mail address has no DNS MX record.

Reject on non FQDN sender

Rejects mail when the client MAIL FROM command is not in the form of an FQDN (Fully Qualified Domain Name), for example, mail.example.com. This option only applies to untrusted mail.

Reject on unauth pipelining

Rejects mail when SMTP commands are sent ahead of the message even though the SMTP server supports pipelining. This option blocks mail from bulk mail software that uses SMTP command pipelining improperly to speed up deliveries.

Reject on missing addresses

Reject mail when no recipients (To:) or sender (From:) were specified in the message headers. These fields are the optional To: and From: fields, not the corresponding Envelope fields.

Reject on missing reverse DNS

Reject mail from a host when the host IP address has no PTR (address to name) record in the DNS, or when the PTR record does not have a matching A (name to address) record.

> ***Warning*** *Many servers on the Internet do not have valid Reverse DNS records. If you set this option, it can result in rejected mail from legitimate sources. We recommend that you do not enable this option.*

2. Click **Apply**.

Reject on Unknown Recipient

The *Reject on Unknown Recipient* feature rejects mail if the intended recipients do not exist locally or in an LDAP directory. Use this option in conjunction with *LDAP Users* and the *LDAP Recipients* feature.

The XCS device determines if a user exists with these checks:

- Checks to see if the user is in the local database of imported *LDAP Users* (Recommended for Active Directory)
- Performs a direct lookup on an LDAP user directory with the *LDAP Recipients* feature

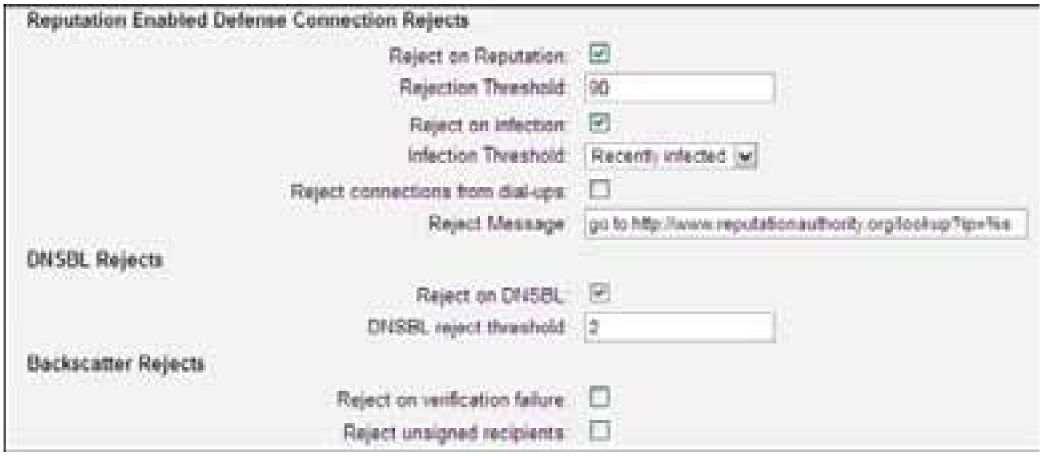
See *Directory Users* for more information on importing LDAP users for user lookups.

See *LDAP Recipients* for information on configuring the LDAP Recipients feature.

> ***Note*** *To override Reject on Unknown Recipient, configure a Specific Access Pattern set to Allow Relaying or Trust.*

Reputation Enabled Defense, DNSBL, and Backscatter Rejects

You can also configure Reputation Enabled Defense, DNS Block Lists, and Backscatter rejects from this page. These features are discussed in more detail later in this section.



Reputation Enabled Defense Connection Rejects

Reject on Reputation: ☑
Rejection Threshold: 90
Reject on infection: ☑
Infection Threshold: Recently infected
Reject connections from dial-ups: ☐
Reject Message: go to http://www.reputationauthority.org/lookup?ip=%s

DNSBL Rejects

Reject on DNSBL: ☑
DNSBL reject threshold: 2

Backscatter Rejects

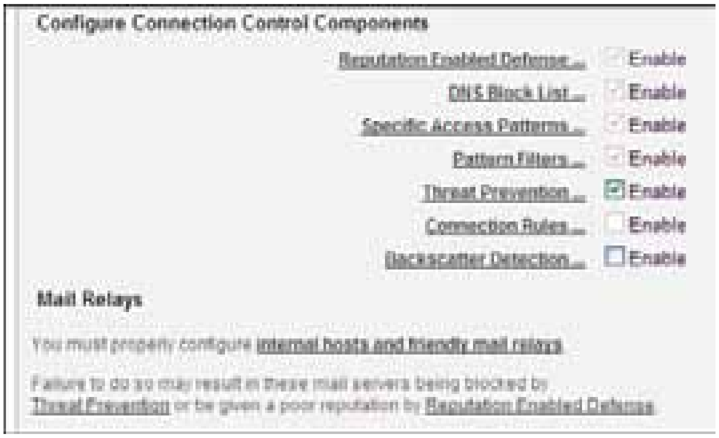
Reject on verification failure: ☐
Reject unsigned recipients: ☐

Connection Control Components

You can enable or disable each Connection Control component depending on your requirements.

To configure the settings for each feature:

1. Select the **Enable** check box for a specific feature.



Configure Connection Control Components

Reputation Enabled Defense ... ☑ Enable

DNS Block List ... ☑ Enable

Specific Access Patterns ... ☑ Enable

Pattern Filters ... ☑ Enable

Threat Prevention ... ☑ Enable

Connection Rules ... ☐ Enable

Backscatter Detection ... ☐ Enable

Mail Relays

You must properly configure internal hosts and friendly mail relays

Failure to do so may result in these mail servers being blocked by Threat Prevention or be given a poor reputation by Reputation Enabled Defense

2. Select the feature link to review or customize the default settings.
3. When finished, click the **Apply** button to save the configuration.

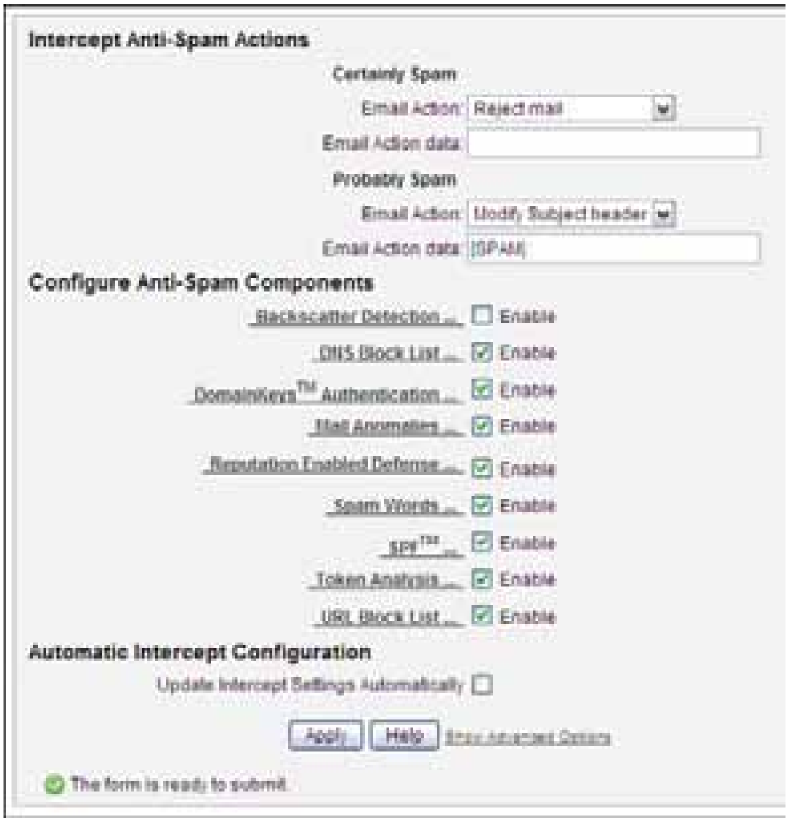
Mail Relays

To trust friendly local networks or addresses of known mail servers in their environment that relay mail through this system, click the **internal hosts and friendly mail relays** link.

You can add specific networks and servers to the relays IP Address list in the Threat Prevention configuration page to prevent them from being blocked by Threat Prevention and RED, as well as make sure that reputation statistics for these addresses are not reported to RED.

Configure Intercept Anti-Spam

Select **Security > Anti-Spam > Anti-Spam** to enable and configure the Intercept Anti-Spam features.



Intercept Anti-Spam Actions

Certainly Spam

Email Action: Reject mail

Email Action data:

Probably Spam

Email Action: Modify Subject header

Email Action data: [SPAM]

Configure Anti-Spam Components

Backscatter Detection ... □ Enable

DNS Block List ... ☑ Enable

DomainKeys™ Authentication ... ☑ Enable

Mail Anomalies ... ☑ Enable

Reputation Enabled Defense ... ☑ Enable

Spam Words ... ☑ Enable

SPF™ ... ☑ Enable

Token Analysis ... ☑ Enable

URL Block List ... ☑ Enable

Automatic Intercept Configuration

Update Intercept Settings Automatically □

The form is ready to submit.

Intercept Anti-Spam Actions

In the *Intercept Anti-Spam Actions* section, you can assign actions for three levels of spam score thresholds.

Certainly Spam

Any message with a score over this threshold (Default: 99) is *Certainly Spam*. These types of messages require a strong action, for example, **Reject Mail** or **Redirect To**.

Probably Spam

Any message with a score over this threshold (Default: 90) is probably spam. This threshold indicates a message with a very high spam score, but not high enough to be *Certainly Spam*. You should treat these messages with a lighter action than *Certainly Spam*, for example, **Redirect To** or **Modify Subject Header**. You should not reject *Probably Spam* messages.

Maybe Spam (Advanced setting)

Any message with a score over this threshold (Default: 60) might be spam but should be treated with caution to prevent false positives. This threshold indicates messages that could be spam, but could also be legitimate mail. We recommend that you use a light action, for example, **Modify Subject Header**.

For each category you can set these fields and actions:

- **Threshold** (advanced view only) – Set the threshold spam score (between 1 and 99) for this category. We recommend that you leave these values at their defaults.

- **Email Action** – Specify one of these actions to take when the threshold is exceeded:
- **Just log** – Log the occurrence, and take no other action.
- **Modify Subject Header** – Insert the specified text in the **Email Action Data** text box into the message subject line.
- **Add header** – Add an “X-” mail header as specified in the **Email Action Data** text box.
- **Redirect to** – Deliver to the mail address or server specified in the **Email Action Data** text box.
- **Discard mail** – Discard the message and do not send a notification to the sender.
- **Reject mail** – Reject the message and send a notification to the sender.
- **BCC** – Send a blind carbon copy of the message to the mail address specified in the **Action Email Data** text box.
- **Quarantine Mail** – Send the message to the administrative quarantine area.
- **Email Action Data** – Select the **Email Action Data** depending on the specified **Email Action**:
- **Modify Subject Header** – Insert the specified text into the subject line, for example, [SPAM]. If this field is left blank, [SPAM] is the default modifier.
- **Redirect to** – Send the message to a mailbox, for example, spam@example.com. You can redirect the message to a spam quarantine, for example, spam.example.com.
- **Add header** – Add an “X-” message header with the specified text, for example, “X-Reject: spam”. The header action data must start with “X-” and must contain a colon followed by a space. If this is not specified, the phrase “X-Reject” is added as a prefix to the header. For example, if you enter “spam”, the full header is “X-Reject: spam”. If enter a header with a colon, for example, “Reason:spam”, the full header is “X-Reason:spam”.

  Leave this field blank to add a default header used by the Intercept Plug-in for Exchange:

  For the *Certainly Spam* action, add the header: X-BTI-AntiSpamCode: certainly

  For the *Probably Spam* action, add the header: X-BTI-AntiSpamCode: probably

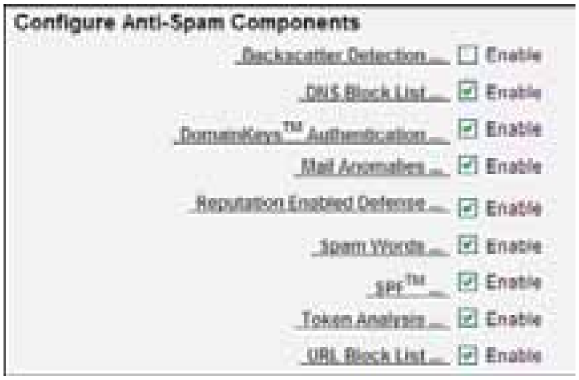
  For the *Maybe Spam* action, add the header: X-BTI-AntiSpamCode: maybe

  For no classification, add the header: X-BTI-AntiSpamCode: none

Configure Intercept Anti-Spam Components

You can enable or disable each component of the Intercept Anti-Spam engine depending on your requirements. To configure the settings for each feature:

1. Select **Security > Anti-Spam > Anti-Spam**.



Configure Anti-Spam Components

Backscatter Detection □ Enable
DNS Block List ☑ Enable
DomainKeys™ Authentication ☑ Enable
Mail Anomalies ☑ Enable
Reputation Enabled Defense ☑ Enable
Spam Words ☑ Enable
SPF™ ☑ Enable
Token Analysis ☑ Enable
URL Block List ☑ Enable

2. Select the **Enable** check box for a specific feature.
3. Select the spam feature link to review or customize the default settings.

4. When finished, click the **Apply** button to save the configuration.

Automatic Intercept Configuration

Select the **Update Intercept Settings Automatically** check box to allow advanced Intercept settings to be updated automatically by WatchGuard. If you use this option, WatchGuard will update your advanced Intercept settings on a periodic basis to make sure you always use the most up-to-date and recommended configuration. Your Intercept actions, thresholds, and component settings are not modified with this option.

> ***Note*** *Automatic Intercept configuration requires that Security Connection be enabled and running.*

This option configures these advanced settings:

- Intercept Component Weights
- Reputation/UBL/DNSBL domains and timeout settings
- Advanced Token Analysis options
- Enable Image Analysis
- Enable PDF Analysis
- Analyze PDF text
- Analyze PDF images
- Enable RTF Analysis
- Legitimate mail and Spam training sources
- Legitimate mail and Spam limits and thresholds
- Dictionary spam count
- Reputation Whitelist

Advanced Intercept Options

Click the **Show Advanced Options** link to display additional advanced Intercept configuration options.

Anti-Spam Header

You can add an Anti-Spam header to a message for diagnostic purposes. The Anti-Spam header contains data on all spam processing applied to the message.

```
X-BTI-
AntiSpam:score:51,sta:51025,dnsbl:off,sw:passed,bsn:none,Brightmail:passed,spf:none,dk:passed,pbmf:n
```

> ***Note*** *You must enable the Anti-Spam header to use the Intercept Plug-in for Exchange.*

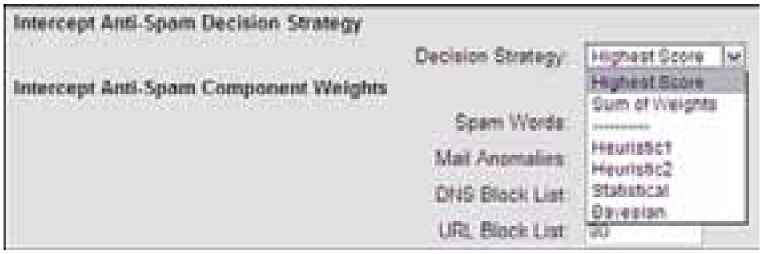
The Anti-Spam header output can contain these items:

Item	Description
score	Overall Intercept score
sta	Token Analysis score
dnsbl	DNS Block List check
sw	Spam Words

Item	Description
bsn	Reputation Enabled Defense reputation
spf	SPF results
brightmail	Brightmail scanning result
dk	DomainKeys results
pbmf	Pattern Based Message Filters
ipr	Mail Anomalies checks
trusted	Trusted or non-trusted
ts	Trusted Senders List
bs	Blocked Senders List
ubl	URL Block List check
bsctr	Backscatter Detection
dfp	Document Fingerprinting

Intercept Decision Strategy

The Intercept Decision Strategy allows administrators to alter the way in which Intercept processes messages for spam.



Intercept Anti-Spam Decision Strategy

Decision Strategy: Highest Score

Intercept Anti-Spam Component Weights

Spam Words:

Mail Anomalies:

DNS Block List:

URL Block List: 30

Highest Score

The Highest Score method uses the maximum score derived from all the scans that are processed. For example, if Mail Anomalies, and DNS Block List are enabled, and DNS Block List results in the highest contributing score for all the scans, then that score is used.

Sum of Weights

The message is initially classified by the Token Analysis and Brightmail scores, and then the weight of any other enabled components with a spam score are added.

> **Note** *The component weights should be adjusted to be lower than their default settings when you use the Sum of Weights decision strategy.*

Heuristic 1

Components are divided into objective and subjective categories. Objective components are DNS Block List, URL Block List, Mail Anomalies, RED Dial-up, SPF, and DomainKeys. Subjective components are Spam Words, Token Analysis, Brightmail, and RED reputation. The message is classified initially by combining the subjective scores and the classification is then adjusted by combining the objective scores. A baseline is established with a subjective filter. If Token Analysis scores a message at 60, a baseline of *Maybe Spam* is established. An additional objective filter that triggers categorizes the message as *Probably Spam*. Two objective filters increases the level to *Certainly Spam*.

Heuristic 2

This strategy is similar to the **Heuristic 1** strategy except that the subjective component scores are weighted more heavily in the final decision than in Heuristic1. In environments where there is no Token Analysis training on outbound legitimate mail (for example, some evaluation scenarios), or for new installations, **Heuristic 2** can result in an increase in false positives. In this case, you should use the **Heuristic 1** strategy, which is identical to **Heuristic 2** except that Token Analysis is de-emphasized and additional Anti-Spam features must be triggered for a message to be considered *Probably Spam* or *Certainly Spam*. When using Intercept for this first time, we recommend that you use **Heuristic 1** until a suitable amount of training has been accumulated before you switch to **Heuristic 2**.

Statistical

Scans are processed independently and the resulting score represents the probability that a message is spam based on statistical computation of the results.

Bayesian

Scans are processed independently and the resulting score represents the probability that a message is spam based on Bayesian computation of the results.

Note *Statistical and Bayesian strategies are experimental, and you should only use these strategies in a test environment.*

Recommended Strategy

We recommend that administrators select the **Heuristic 1** decision strategy. This is a passive strategy that is effective for most environments and provides an excellent spam catch rate with a very low chance of false positives.

Training Period

Depending on the amount of mail sent and received in your environment, it can take several days of mail processing and training to properly adjust the default training database for the content of your organization's mail flow. At least 500 legitimate mail messages and 1000 spam messages must be processed to accurately train the WatchGuard XCS.

When the initial training period is complete, you can modify the Intercept Anti-Spam decision strategy from the default **Heuristics 1** to **Heuristics 2**. The **Heuristics 2** decision strategy puts more emphasis on your trained mail to help identify spam messages and to prevent false positives (legitimate mail classified as spam).

> ***Warning*** *Choosing the wrong strategy for your environment could result in false positives and a lower spam capture rate.*

Intercept Component Weights

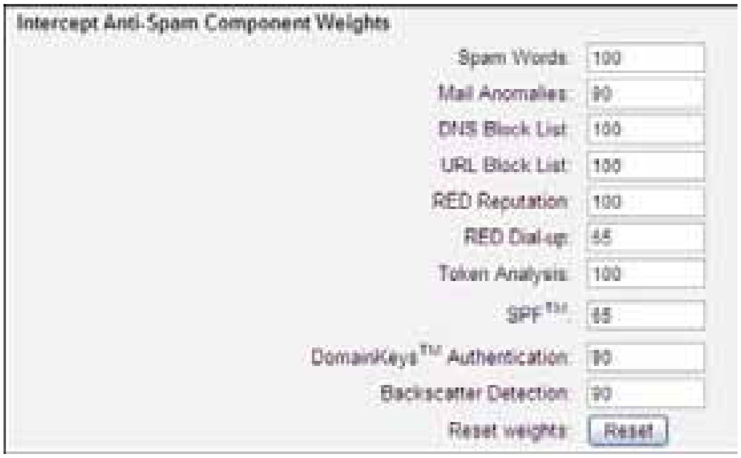
To customize the Intercept engine, configure the weights for each Intercept component that help determine the final spam score for a message. These values represent the scores used if that component triggers. For example, if a mail message triggers a DNS Block List, the spam score contribution for that message is the defined weight, for example, 100.

The final result of these scores is decided by your selected Decision Strategy, for example, **Highest Score** or **Heuristic 2**. Valid weights for each component are from 0 to 100. Set the weight to 0 if you want that feature to have no bearing on the final spam score of a message. Set this value to 100 if you want this component to have a strong weight on the final spam score of a message.

> ***Warning*** *We recommend you do not modify the default component weights. Weight misconfiguration can cause a degradation in your Anti-Spam capture rate.*

To configure Anti-Spam component weights:

1. Select **Security > Anti-Spam > Anti-Spam**.



Intercept Anti-Spam Component Weights

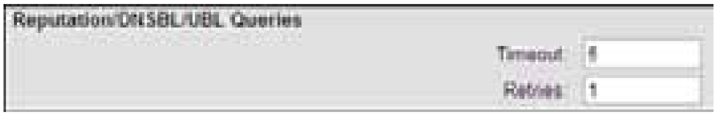
Spam Words:	100
Mail Anomalies:	90
DNS Block List:	100
URL Block List:	100
RED Reputation:	100
RED Dial-up:	45
Token Analysis:	100
SPF™:	65
DomainKeys™ Authentication:	90
Backscatter Detection:	90
Reset weights:	Reset

2. Set the weight for each component.
   A value of 0 means that the component is a completely unreliable indicator of spam. A value of 100 means that this component is a completely reliable indicator of spam.
3. Click **Apply**.

Reputation/DNSBL/UBL Timeout Setting

Reputation Enabled Defense, DNS Blocks lists, and URL Block Lists, if enabled, perform their own separate checks per message when they scan messages for spam. In the event that one or more of the specified services are unavailable, the query to the service domain times out.

These options allow you to configure the timeout and retry settings for each lookup query. We recommend that you use the system defaults. If a query for Reputation Enabled Defense, DNS Blocks Lists, or URL Block Lists exceeds the timeout and retry threshold, the checks for this message are skipped for that feature.



Reputation/DNSBL/UBL Queries

Timeout: 5

Retries: 1

- **Timeout** – The delay (in seconds) between each retry in the event of a Reputation/DNSBL/UBL lookup failure for a message. The default is 5 seconds.
- **Retries** – The number of retries to perform in the event of a Reputation/DNSBL/UBL lookup failure for a message. The default is 1 retry.

Intercept Plug-in for Exchange

The Intercept plug-in is installed on a Microsoft Exchange 2003 server to assign processed messages from the WatchGuard XCS an SCL (Spam Confidence Level) rating. The SCL rating is used by Exchange to classify messages in terms of how likely they are to be spam. The rating is based on a scale from 0 to 9, where 9 indicates the message is most likely spam, and 0 indicates a legitimate message. Each Intercept feature provides information (via the Anti-Spam header) to the Intercept plug-in running on the Exchange server and maps the Intercept Anti-Spam score values to an equivalent SCL rating. When the SCL rating for a message is determined, a configurable action is performed depending on the thresholds set in the plug-in.

You can set a **Gateway Blocking Threshold** to perform an action on a message before it is delivered to a user's inbox on their Outlook client. You can discard (with no notification) or reject (with notification) the message, or take no action. This allows you to stop the delivery of messages with very high SCL ratings.

We recommend that you do not reject mail at the Exchange level. You should set the action for the **Gateway Blocking Threshold** to be **No Action**, and then set an appropriate **Store Threshold** to allow the end users to manage their spam and legitimate mail with the Outlook mail client's Junk Email Folder. You should reject messages with very high spam scores at the WatchGuard XCS level.

You can configure a separate **Store Threshold** that sets a specific SCL rating value where messages equal to or above this rating are automatically delivered to a user's Junk Email folder instead of the inbox on their Outlook client. Also, user's of the Outlook and OWA 2003 client can define Safe Senders and Blocked Senders to trust and block email addresses and domains.

You can download the Intercept Plug-in for Exchange from the link on the main Intercept Anti-Spam page. You can also obtain the Plug-in from the WatchGuard support site.

The Intercept Plug-in for Exchange requires these versions of software:

- Microsoft Windows 2000 (or greater) Server
- Microsoft Exchange 2003 (SP1 or SP2. The plug-in should be installed on the Front End or Bridge Head server, not a back end server). Please see the *Intercept Plug-in for Exchange Installation and User Guide* for detailed instructions on how to install and configure the plug-in.

For Microsoft Exchange 2007 or greater, see the WatchGuard Knowledge base for information on how to use Exchange Transport Rules with the WatchGuard XCS.

Spam Words

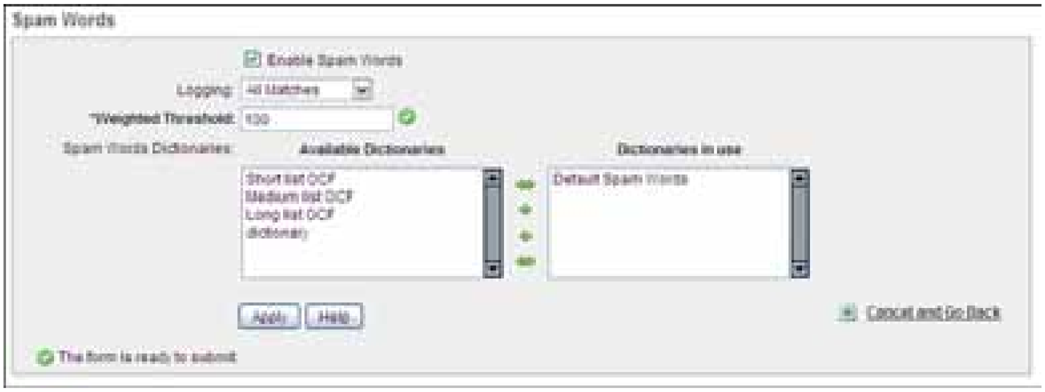
The WatchGuard XCS provides a Spam Words dictionary filter. When enabled, all inbound messages passing through the XCS device are scanned for words and phrases that appear in the spam words dictionary. Messages with words or phrases in their subject or body that match the phrase list are more likely to be spam. The Intercept Anti-Spam engine uses this information to help decide if the message is spam or legitimate mail.

The WatchGuard XCS includes a basic pre-configured spam words list for message filtering. WatchGuard's default list includes basic words most commonly found in spam, for example, "prescription" and "viagra". You can view and modify the full default list. You can use this list to build and upload your own custom spam word list.

> **Note** *We recommend that you review this default spam words list to make sure any included words are not part of their organizations functions. For example, remove the word "prescription" if your organization is involved with the pharmaceutical industry.*

To configure Spam Words:

1. Select **Security > Anti-Spam > Anti-Spam**.
2. Select **Spam Words**.
   The Spam Words page appears.



Spam Words

☑ Enable Spam Words

Logging: All Matches

*Weighted Threshold: 100

Spam Words Dictionaries:

Available Dictionaries	Dictionaries in use
Short list OCF Medium list OCF Long list OCF (dictionary)	Default Spam Words

The form is ready to submit

3. Select the **Enable Spam Words** check box.
4. From the **Logging** drop-down list, select the method to log messages that contain matched spam words and phrases.

   The logging information appears in the *Mail Logs*:

- **No logging** – Perform no logging.
- **First match only** – Display only the first matching word.
- **All matches** – Display all matched words.

4. In the **Weighted Threshold** text box, type the threshold for weighted spam words dictionaries.

   If you use a weighted spam dictionary, the terms and their weight in the dictionary must match or exceed this threshold to classify a message as spam. If you use both weighted and unweighted dictionaries, the final action is performed if the sum of the weights exceeds the configured weighted threshold, or if a match occurs in an unweighted dictionary. See *Dictionaries and Lists* for more details on weighted dictionaries.

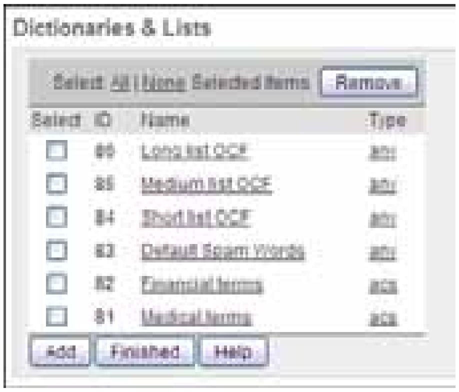
5. In the **Spam Words Dictionaries** section, select the dictionaries to use for Anti-Spam checks.

   The dictionaries available are listed in the *Available Dictionaries* list. Use the arrow buttons to move the dictionaries to the *Dictionaries in Use* list as required. You can use the *Default Spam Words* list provided by WatchGuard, or you can upload a custom list in **Security > Content Control > Dictionaries & Lists**.

Add a Spam Words Dictionary

To add a Spam Words dictionary:

1. Select **Security > Content Control > Dictionaries & Lists**.
   The Dictionaries & Lists page appears.



Dictionaries & Lists

Select: All | None Selected items [Remove]

Select	ID	Name	Type
□	86	Long list OCF	any
□	85	Medium list OCF	any
□	84	Short list OCF	any
□	83	Default Spam Words	any
□	82	Financial terms	acs
□	81	Medical terms	acs

[Add] [Finished] [Help]

2. Select the **Default Spam Words** list.
   The default list contains a list of common words that are typically seen in spam messages.
3. Click **Download** to save and view the text file of spam words.

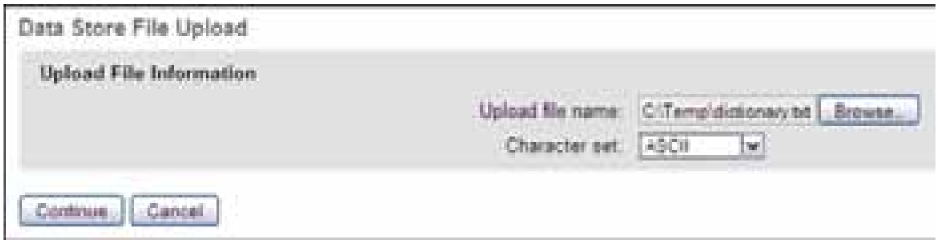
   The list contains one word or phrase per line.

   For example,

   `free picfree picsfree piczmedsmedz`

   You can edit this base list to create your own dictionary of spam words, and delete default words that are not required.

4. Select **Security > Content Control > Dictionaries & Lists**.
5. Click **Add**.
6. Click **Browse**.
7. Click **Continue**.



Data Store File Upload

Upload File Information

Upload file name: C:\Temp\dictionary.txt

Character set: ASCII

The file information page displays the initial contents of the file where you can change the name of the list and the type of dictionary.

8. From the **Type** drop-down list, select **spam**.

   This indicates that you can use the dictionary file with the Spam Words feature. Select **Any** to use the dictionary with any dictionary-based scanning feature. Use the *Weight* option for Weighted Dictionaries.

9. Click **Continue**.
   The new dictionary appears in the list and you can select it when you use Spam Words.

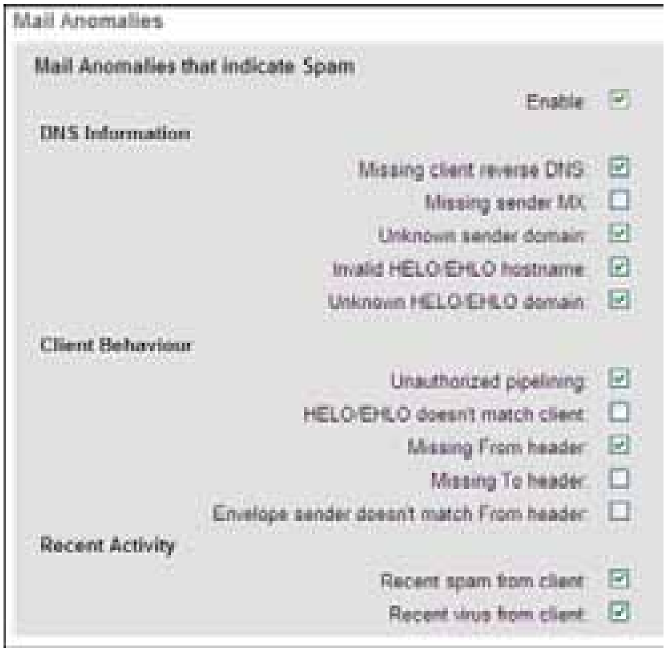
Mail Anomalies

The Mail Anomalies feature performs checks on incoming messages to help determine whether the message is coming from a known source of spam or is legitimate mail. Servers that send spam have certain characteristics that can give away the nature of the sending system. Many spammers deploy scripts and use spoofed or false information when they send mail. The WatchGuard XCS can check incoming connections for patterns of these behaviors to help determine whether mail from an incoming server is legitimate or spam.

The Mail Anomalies feature checks messages for a variety of information that can reveal discrepancies between the message's sending host and the host listed in the message envelope and contents, and information about messages recently sent by the sending host. A message must fail four or more checks to be considered spam.

To configure Mail Anomalies:

1. Select **Security > Anti-Spam > Anti-Spam > Mail Anomalies**.
   The Mail Anomalies page appears.



Mail Anomalies

Mail Anomalies that indicate Spam

Enable ☑

DNS Information

Missing client reverse DNS ☑

Missing sender MX □

Unknown sender domain ☑

Invalid HELO/EHLO hostname ☑

Unknown HELO/EHLO domain ☑

Client Behaviour

Unauthorized pipelining ☑

HELO/EHLO doesn't match client □

Missing From header ☑

Missing To header □

Envelope sender doesn't match From header □

Recent Activity

Recent spam from client ☑

Recent virus from client ☑

2. The WatchGuard XCS can detect these types of anomalies:

   These checks relate to issues with DNS record lookups for the sending host:

   - **Missing client reverse DNS** – Checks to see if the sending host has a PTR (address to name) record and the PTR record has a matching A (name to address) record.
   - **Missing sender MX** – Checks to see if the sender mail address has a DNS MX record. This check is more restrictive than the check for Unknown sender domain. If Unknown sender domain fails then this check also fails. We recommend that you only use one of the two checks at the same time.
   - **Unknown sender domain** – Checks to see if the sender mail address has a DNS A or MX record. This check is less restrictive than the check for **Missing sender MX**. If this check fails, then **Missing sender MX** also fails. We recommended that you only use one of these two checks at the same time.
   - **Invalid HELO/EHLO hostname** – Checks to see if the HELO/EHLO address is a valid hostname.
   - **Unknown HELO/EHLO domain** – Checks to see if the HELO/EHLO address has a DNS A or MX record.

   These checks relate to issues with the connecting client's SMTP connection and message information:

   - **Unauthorized pipelining** – Checks to see if the client sends SMTP commands ahead of time without knowing that the mail server actually supports SMTP command pipelining. This check detects bulk mail software that improperly uses SMTP command pipelining to speed up deliveries.
   - **HELO/EHLO doesn't match client** – Checks to see if the HELO/EHLO address matches the sending host address.
   - **Missing From header** – Checks to see if the From header is present.
   - **Missing To header** – Checks to see if the To header is present.

- **Envelope sender doesn’t match From header** – Checks to see if the From header matches the envelope sender address.

These checks identify clients who have recently sent spam or viruses and only work if you enable Threat Prevention (configured in **Security > Anti-Spam > Threat Prevention**.)

- **Recent spam from client** – Checks to see if the sending host recently sent spam.
- **Recent virus from client** – Checks to see if the sending host recently sent a virus.

If a message fails four or more checks, the weight assigned to Mail Anomalies in the Intercept settings is the score used for Intercept processing.

3. Click **Apply**.

DNS Block Lists

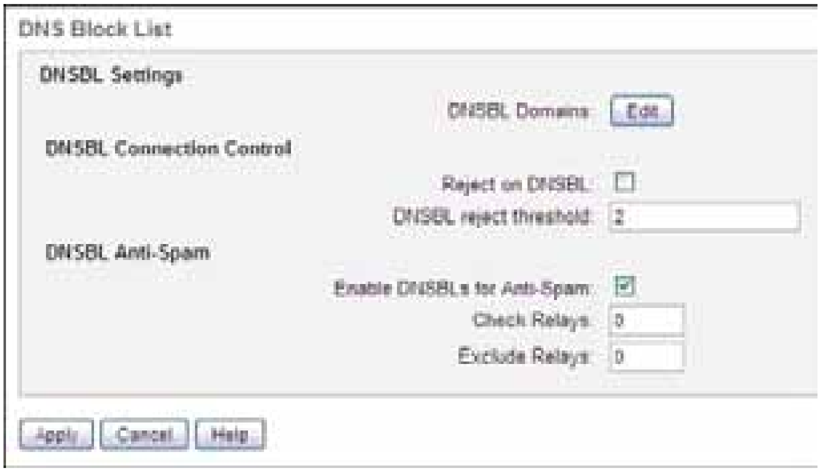
DNS Block Lists (DNSBL) contain the addresses of known sources of spam and are maintained by both commercial and non-commercial organizations. The lookup mechanism is DNS-based that results in a lookup on the specified DNSBL server for every server that attempts to connect to the WatchGuard XCS.

The weight assigned to DNS Block Lists in the Intercept settings is the score used by Intercept processing when a DNSBL triggers for a message. If a sender is matched on more than one DNS Block List, this increases the weight score assigned by Intercept for each list on which it is matched.

> ***Note*** *If a message that you want to receive is blocked by a DNSBL, add a Specific Access Pattern to trust messages from that client.*

To configure DNS Block Lists:

1. Select **Security > Anti-Spam > Anti-Spam**.
2. Select **DNS Block List**.
   The DNS Block List page appears.



DNS Block List

DNSBL Settings

DNSBL Domains: Edit

DNSBL Connection Control

Reject on DNSBL: ☐

DNSBL reject threshold: 2

DNSBL Anti-Spam

Enable DNSBLs for Anti-Spam: ☑

Check Relays: 0

Exclude Relays: 0

3. To reject mail from blocked clients regardless of other message processing, select the **Reject on DNSBL** check box.

> ***Warning*** *Reject on DNSBL rejects the message at SMTP connection time regardless of other Intercept processing. Use caution when you enable this feature.*

4. In the **DNSBL Reject Threshold** text box, type the number of block lists on which the server must be listed before you reject a message.
   If this value is set to 2 (default) the server must appear on at least two DNSBLs before it is rejected.
5. To use DNSBLs in the Intercept Anti-Spam decision, select the **Enable DNSBLs for Anti-Spam** check box.
6. In the **Check Relays** text box, type how many relay points, starting from the latest headers to the earliest, should be checked against a DNS Block List.

   The **Check Relays** setting deals with spammers who are relaying their messages through an intermediate server. The information about the originating server is carried in the headers of the message. Acceptable values are between “0” and “ALL”. We recommend that you leave this option at the default value of “0”.

   > ***Note*** *You must enable the Check Relays option if the WatchGuard XCS is behind another MTA or mail gateway. This action makes sure that the relay before the intermediary MTA is checked.*

7. In the **Exclude Relays** text box, type how many received headers to exclude from DNSBL checks, starting from the earliest to the most recent.

   Some ISPs include the originating dial-up IP as the first relay point. This can result in blocking dial-ups that are legitimate servers. We recommend you set this value to “1” or “0”. Use “1” if any of the DNSBL servers utilized include dynamic IP addresses (for example, a dial-up connection). If the DNSBL service does not include dial-ups, set this to “0” to make sure you do not reject mail originating from web mail systems.

   This is an example of using the **Check Relays** and **Exclude Relays** options:

   Server A -> Server B -> Server C -> Server D -> WatchGuard XCS

   With the mail relayed through four previous servers (A-D), the received headers of a message appear in this order:

   Received: D
   Received: C
   Received: B
   Received: A

   With **Check Relays** enabled, the system starts with server D and checks the configured number of received headers. If **Check Relays** is set to “3”, it checks D, C, and B.

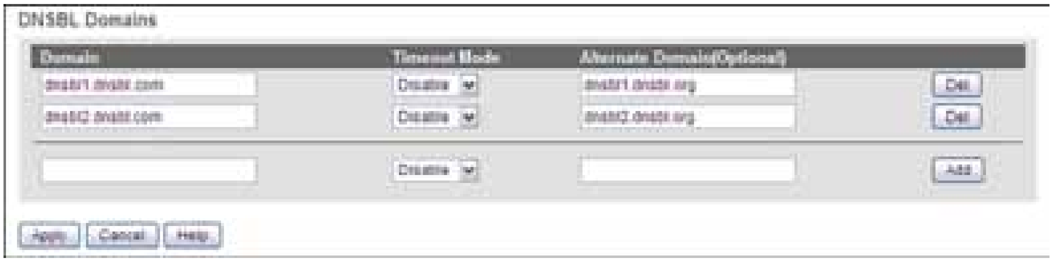
   Select the **Exclude Relays** option to ignore the configured number of received headers starting at the end of the header list, regardless of what the **Check Relays** option is set to. If **Exclude Relays** is set to “1”, then server A is excluded from the checks.

8. Click **Apply**.

DNSBL Servers

To edit the list of DNS Block List servers:

1. Click **Edit**.



DNSBL Domains

Domain	Timeout Mode	Alternate Domain(Optional)	
dnsbl1.dnsbl.com	Disable	dnsbl1.dnsbl.org	Del
dnsbl2.dnsbl.com	Disable	dnsbl2.dnsbl.org	Del
	Disable		Add

2. Click **Apply** when finished.

> ***Note*** *Do not modify the default WatchGuard DNSBL servers.*

Timeout Mode

The *Timeout Mode* allows the timely recovery of lookup timeouts to the DNSBL domain and improves redundancy with alternate DNSBL domains in the event the primary domain is unavailable. If you cannot contact the primary or alternate DNSBL domains, the DNSBL check is skipped for the message. An alarm also triggers to notify you if the system cannot contact a service.

- **Disable** – Do not perform DNSBL lookups if the DNSBL domain is unavailable. The system checks the status of the domain every 5 minutes. Domain queries resume when the service is available again.
- **Alternate** – Use the alternate DNSBL domain specified in the *Alternate Domain* field. The system checks the status of the primary domain every 5 minutes. The system reverts to the primary domain when the primary domain service is restored.
- **Ignore** – Continue to attempt a lookup to the DNSBL domain. If the system exceeds the timeout threshold (900 seconds), trigger an alarm and skip the query.

URL Block Lists

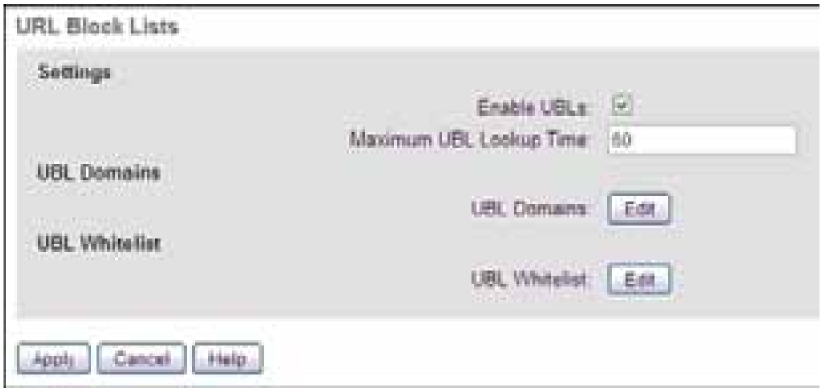
URL Block Lists contain a list of domains and IP addresses of URLs that have appeared previously in spam, phishing, or other malicious messages. This feature examines a message for any URLs contained in the body to see if they appear on a block list.

Similar to DNS Block Lists, the WatchGuard XCS queries the URL Block List to see if a URL exists on the configured block list server. If a match is found, this information is used by the Intercept engine to decide whether a message is spam or legitimate mail.

If the URL in a message is matched on a URL Block List, it is assigned a score as per the URL Block List weight configured in the Intercept component weight setting. If a URL is matched on more than one URL Block List, this increases the weight of the score assigned by Intercept for each list on which it is matched.

To configure URL Block Lists:

1. Select **Security > Anti-Spam > Anti-Spam**.
2. Select **URL Block List**.
   The URL Block Lists page appears.



URL Block Lists

Settings

Enable UBLs: ☑

Maximum UBL Lookup Time: 60

UBL Domains

UBL Domains: Edit

UBL Whitelist

UBL Whitelist: Edit

3. Select the **Enable UBLs** check box.
4. In the **Maximum UBL Lookup Time** text box, type the maximum time (in seconds) for a lookup to a URL Block List.

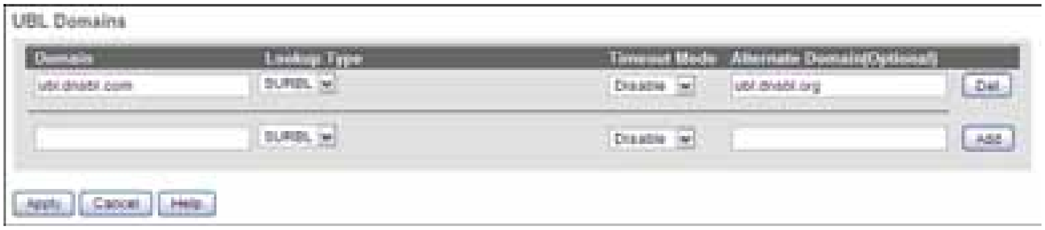
   This option prevents excessive processing time for messages that contain a large number of URLs. If all of the URLs in a message cannot be looked up before the timeout value is reached, the checks stop and only the URLs checked within the time limit are used in the Intercept Anti-Spam decision. Valid values are from 1 to 3600. The default is 60 seconds.
5. Click **Apply**.

UBL Domains

You can check URLs with a SURBL (Spam URI Realtime Block Lists) method that performs lookups for a domain with the base domain or IP addresses of the URL, or a DNSBL lookup that can query a DNS Block List server to lookup the full domain with the resolved host IP address for the URLs in a message.

WatchGuard provides a default SURBL server that you can use for the URL Block List. You can add other SURBL or DNSBL lists, but you must use caution when you add servers because some free services can introduce false positives.

Click the **Edit** button to configure the SURBL and DNSBL server lists.



UBL Domains

Domain	Lookup Type	Timeout Mode	Alternate Domain(Optional)	
ubl.dnsbl.com	SURBL	Disable	ubl.dnsbl.org	Del
	SURBL	Disable		Add

Timeout Mode

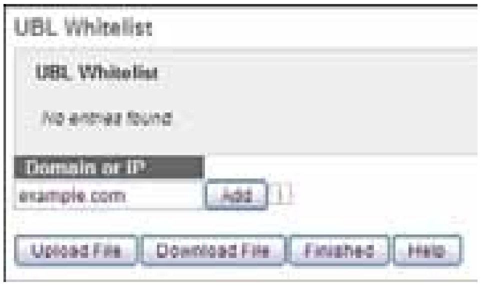
The *Timeout Mode* allows for the timely recovery of lookup timeouts to the UBL domain and improves redundancy with alternate UBL domains in the event the primary domain is unavailable. If you cannot contact the primary or alternate UBL domains, the UBL check is skipped for the message. An alarm also triggers to notify you if the system cannot contact a service.

- **Disable** – Do not perform UBL lookups if the UBL domain is unavailable. The system checks the status of the domain every 5 minutes. Domain queries resume when the service is available again.
- **Alternate** – Use the alternate UBL domain specified in the *Alternate Domain* field. The system checks the status of the primary domain every 5 minutes. The system reverts to the primary domain when the primary domain service is restored.
- **Ignore** – Continue to attempt a lookup to the UBL domain. If you exceed the timeout (900 seconds), trigger an alarm and skip the query.

UBL Whitelist

You can define a list of trusted domains and IP addresses that bypass URL Block List scanning, even if messages from those addresses contain URLs that appear in a URL Block List.

1. Click the **Edit** button to configure the UBL Whitelist.
2. Type a domain name or IP address to trust, then click **Add**.
3. If you enter a domain (for example, example.com), all subdomains of that domain are included (for example, www.example.com).



UBL Whitelist

UBL Whitelist

No entries found

Domain or IP: example.com

Upload and Download Lists

You can upload a list of domain names and IP addresses in one text file. The entries must appear one per line in this format:

```
example.com
example2.com
example3.com
192.168.1.100
```

You must use a text editor to create the file ubl_wl.csv.

To update a UBL file:

1. To download the UBL list from the WatchGuard XCS, click **Download File**.
2. Open the file and update the UBL list.
3. Click **Upload File** and upload the edited file to the WatchGuard XCS.

Reputation Enabled Defense (RED)

Reputation Enabled Defense provides connection-level security for email and web through a reputation lookup that scores mail servers and web site URLs as good, bad, or unknown/neutral. The lookup relies on a powerful, cloud-based reputation database that aggregates data from multiple feeds, including industry-leading block lists and Anti-Virus engines.

The WatchGuard XCS uses this information to either reject the message immediately or contribute to the Intercept score if a message is detected from a source with a poor reputation or numerous virus infections.

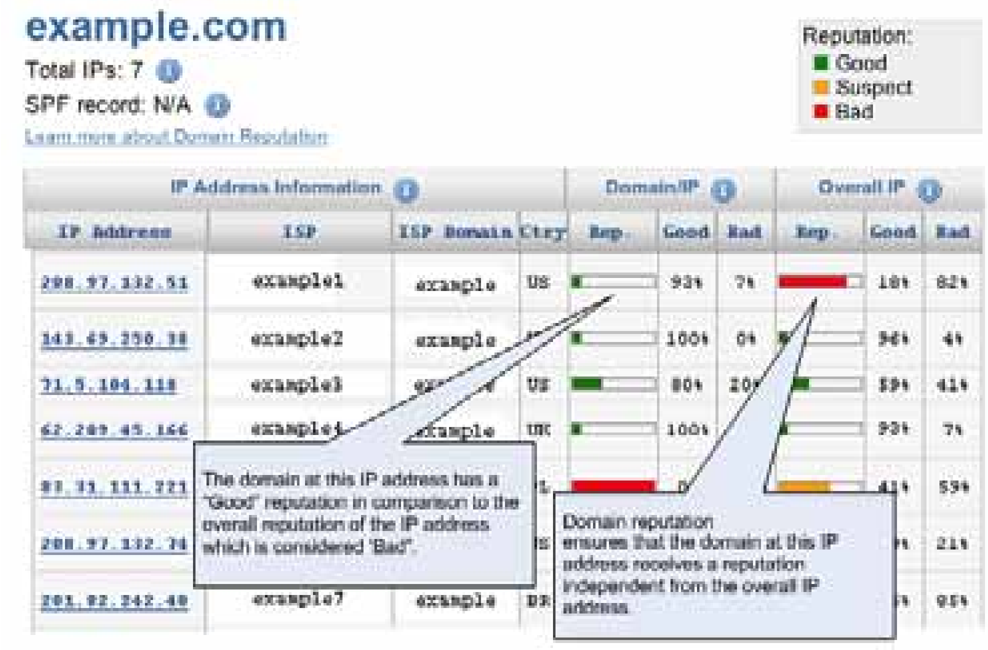
If you enable Reputation Enabled Defense, the WatchGuard XCS queries for statistics from the RED service for the sender IP of each message received, excluding those from trusted and known networks. With the information returned from RED, the XCS can make a decision about whether a message is spam or legitimate mail. A reputation closer to “0” indicates the sender is extremely reliable and rarely sends spam or viruses. A reputation closer to “100” indicates the sender is extremely unreliable and often sends spam or viruses. An IP address with no previous information from any source is assigned an initial neutral value of “50”.

Reputation Whitelists allow you to train on messages from known legitimate sources based on their reputation.

Domain and Sender Reputation

Domain and Sender Reputation increases the reputation effectiveness to examine not only the IP reputation of a sender, but also the domain name and envelope sender information from that IP address. A domain can receive a reputation independent of the behavior of another domain originating from the same address.
A specific sender address receives a reputation independent of the behavior of another sender address from the same domain or IP address. For a message from the sender user@example.com, a query is sent to RED to check the sender address user@example.com, the domain example.com, and the originating IP address of the connection.

RED examines the behavior of the user at its originating IP address (user@example.com, 207.236.65.232), and also the domain at its originating IP address (example.com, 207.236.65.232). The result generated by RED depends on the reputation for that specific sender at that IP address, on the reputation of the domain originating from that IP address, and on reputation of the IP address itself. If there is enough information to make a decision on the reputation of a specific sender at that IP address (user@example.com, 207.236.65.232), RED does not make use of the information on the domain and IP address reputation. If there is enough information to make a decision on the reputation of a domain at that IP address (example.com, 207.236.65.232), RED does not make use of the information on the IP address reputation. If there is no recorded reputation information on a specific sender address or domain, RED uses the reputation of the IP address.



example.com

Total IPs: 7

SPF record: N/A

Learn more about Domain Reputation

Reputation:
🟩 Good
🟧 Suspect
🟥 Bad

IP Address Information				Domain/IP			Overall IP		
IP Address	ISP	ISP Domain	Ctry	Rep.	Good	Bad	Rep.	Good	Bad
208.97.132.51	example1	example	US	🟩	93%	7%	🟥	18%	82%
143.69.250.38	example2	example		🟩	100%	0%	🟩	96%	4%
71.5.104.118	example3	ex	US	🟩	80%	20%	🟩	59%	41%
62.209.45.166	example4	example	UK	🟩	100%		🟩	93%	7%
83.31.111.221			L	🟥	0		🟧	41%	59%
208.97.132.74			S						21%
201.82.242.40	example7	example	DE						95%

The domain at this IP address has a "Good" reputation in comparison to the overall reputation of the IP address which is considered "Bad".

Domain reputation ensures that the domain at this IP address receives a reputation independent from the overall IP address.

The Domain and Sender Reputation query and any uploaded information is sent to the RED network as a one-way hash that cannot be reversed. All information shared with RED is encrypted to protect the details of the domain and sender. If you disable this option, only the IP address reputation is used when you query and share statistics with RED.

Reputation Enabled Defense statistics sharing

These statistics are sent to the RED network when **Share Statistics** is enabled:

- Originating IP address
- Destination IP address
- Total mail
- Clean mail
- Spam mail (this includes results of Intercept scanning)
- Anti-virus scanning results
- Outbreak control results
- Known and unknown recipients
- Malformed mail
- Domain and user information (sent using a one-way hash for security purposes)
- Checksum identification of attached files

> ***Note*** *Reputation service queries use the DNS protocol on UDP port 53. Statistics sharing uploads data to the reputation network using HTTPS on TCP port 443. You must open up these ports on your network firewall if the system is located behind the firewall.*

Trusted Clients and Known Mail Servers

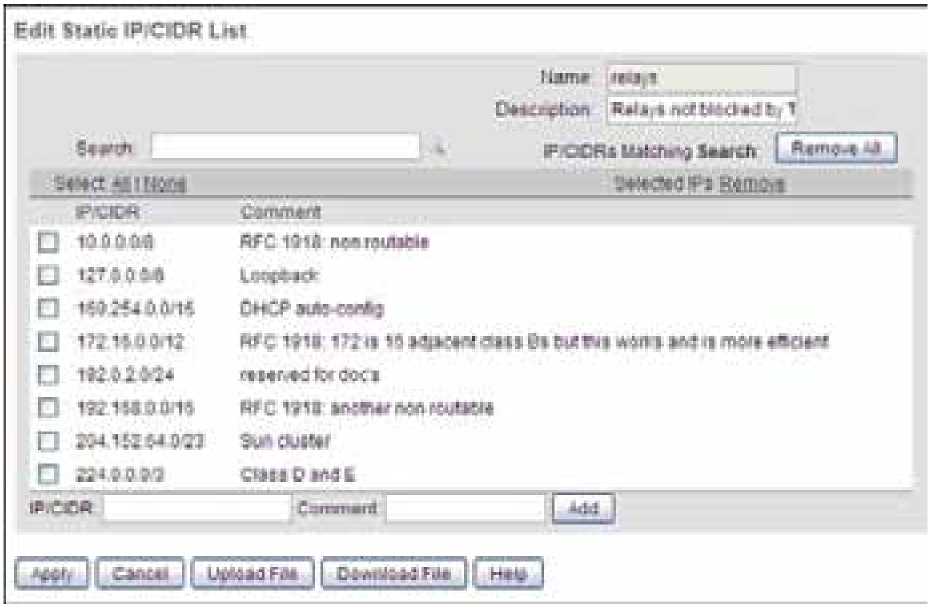
You can trust friendly local networks or addresses of known mail servers in their environment that relay mail through this system. To trust specific networks and servers, add them to the *relays* IP Address list in the Threat Prevention configuration page to prevent them from being blocked by Threat Prevention and RED, as well as make sure that reputation statistics for these addresses are not reported to RED.

For example, in certain environments with a backup MTA (Mail Transfer Agent) server, the backup system may be classified with a poor reputation because the mail received from the backup includes relayed spam. If the WatchGuard XCS is offline, mail is collected by the backup MTA as specified in the organization's MX records. When the WatchGuard XCS comes back online, this mail (which may include spam, viruses, and other types of infected mail) is forwarded from the backup MTA to the WatchGuard XCS for processing. If RED is enabled, this backup system may receive a low reputation score from RED.

Reputation Enabled Defense checks and statistics sharing are not performed for any internal IP addresses and systems listed in the *Relays* list. If a message comes from an IP address identified in the *Relays* list and **Share Statistics** is enabled, an upload of information can still occur. If a prior network hop is listed in a Received header, it is considered the source of the message and an upload occurs as if that IP address had sent it directly. Each system in the Received header is consulted until a suitable one is found. Identified relays and internal IP addresses are ignored.

To add a system to the *relays* list:

1. Select **Security > Anti-Spam > Reputation Enabled Defense**.
2. Click the **internal hosts and friendly mail relays** link.
   The relays Static IP/CIDR List page appears.



Edit Static IP/CIDR List

Name: relays

Description: Relays not blocked by T

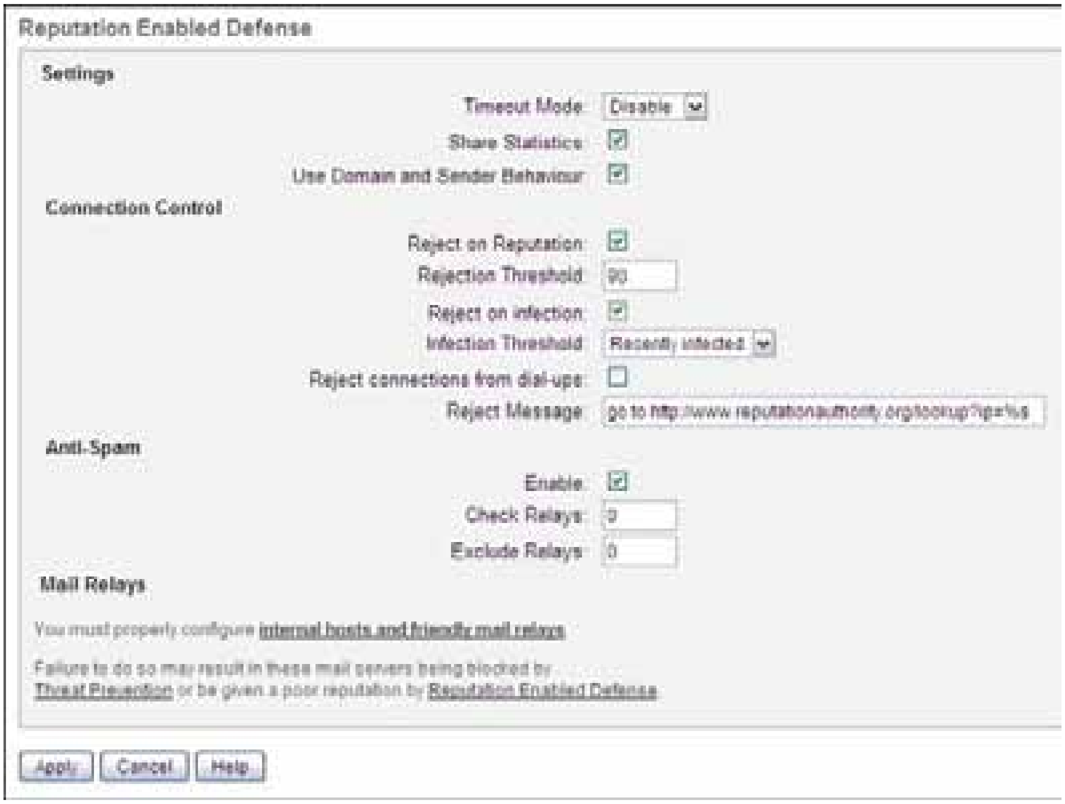
	IP/CIDR	Comment
□	10.0.0.0/8	RFC 1918: non routable
□	127.0.0.0/8	Loopback
□	169.254.0.0/16	DHCP auto-config
□	172.16.0.0/12	RFC 1918: 172 is 16 adjacent class Bs but this works and is more efficient
□	192.0.2.0/24	reserved for doc's
□	192.168.0.0/16	RFC 1918: another non routable
□	204.152.64.0/23	Sun cluster
□	224.0.0.0/3	Class D and E

3. Add the address of an internal relay.
4. Click **Add**.

Configure Reputation Enabled Defense Checks

To configure Reputation Enabled Defense:

1. Select **Security > Anti-Spam > Reputation Enabled Defense**.
   The Reputation Enabled Defense page appears.



Reputation Enabled Defense

Settings

Timeout Mode: Disable

Share Statistics: ☑

Use Domain and Sender Behaviour: ☑

Connection Control

Reject on Reputation: ☑

Rejection Threshold: 90

Reject on infection: ☑

Infection Threshold: Recently infected

Reject connections from dial-ups: ☐

Reject Message: go to http://www.reputationauthority.org/lookup?ip=%s

Anti-Spam

Enable: ☑

Check Relays: 0

Exclude Relays: 0

Mail Relays

You must properly configure internal hosts and friendly mail relays

Failure to do so may result in these mail servers being blocked by Threat Prevention or be given a poor reputation by Reputation Enabled Defense

2. From the **Timeout Mode** drop-down list, select a timeout mode to use in the event the primary domain is unavailable.

   In the event the primary RED domain is unavailable and the timeout mode is set to **Alternate**, an alternate RED domain is queried. If the primary or alternate RED domains cannot be contacted, the RED check is skipped for the message. An alarm triggers to notify you if you cannot contact service.

   - **Disable** – No RED lookups are performed if the RED domain is unavailable. The system checks the status of the domain every 5 minutes. Domain queries resume when the service becomes available.
   - **Alternate** – Use an alternate RED domain for queries. The system checks the status of the primary domain every 5 minutes. The system reverts to the primary domain when the primary domain service is restored. You cannot modify the alternate RED domain.
   - **Ignore** – Continue to attempt a lookup to the RED domain. The query is skipped and an alarm triggers if you exceed the timeout threshold (900 seconds).

3. To share Reputation Enabled Defense information, for example, spam and virus statistics for connecting client IP addresses, from this XCS device with the RED network, select the **Share Statistics** check box.

> ***Note*** *You must enable TCP Port 443 outbound to upload statistics to the reputation server. There are no security risks associated with sharing statistics. The XCS device does not relay any private or sensitive information to the Reputation Enabled Defense service.*

4. To use domain and sender behavior when you perform Reputation Enabled Defense checks, select the **Use Domain and Sender Behaviour** check box.
   This option increases the effectiveness of RED by examining not only the IP reputation of a sender, but also the domain name and envelope sender information from that IP address.
5. To reject messages from senders whose reputation is above the configured **Reputation Threshold**, select the **Reject on Reputation** check box.

   A reputation closer to “0” indicates the sender is extremely reliable and rarely sends spam or viruses.
   A reputation closer to “100” indicates the sender is extremely unreliable and often sends spam or viruses. An IP address with no previous information from any source is assigned an initial neutral value of “50”.

   To override a RED reject, add the server to the internal hosts and friendly mail relays list. You can also override RED rejects with a Specific Access Pattern set to **Trust** the rejected address. You cannot override RED rejects with a policy.

   You can also use a Pattern Filter set to **Bypass** (to bypass all Anti-Spam and content checks), **Trust** (to accept and train as valid mail) or **Accept** (just accept without training) the message. This may interfere with later message processing and we recommend you use the mail relays list.
6. In the **Rejection Threshold** text box, type a threshold over which a message is rejected.

   The default value is “90”. If the reputation of a connecting system is greater than this value, it is rejected. The lower the reputation threshold, the greater the chance that a system with valid mail is blocked. This setting is only valid when you enable **Reject on Reputation**.
7. To reject messages from senders based on the criteria configured in the **Infection Threshold** option, select **Reject on Infection**.
8. From the **Infection Threshold** drop-down list, select the criteria for rejecting messages based on whether the sending host is **Currently infected** (received in last hour), or **Recently infected** (received in last day).
   This is setting is only valid when you enable Reject on Infection.
9. To reject messages sent directly from dial-up connection, select the **Reject Connection From Dial-ups** check box.

> ***Note*** *If a message is not rejected because it violates a reputation threshold, the reputation score and information about whether the sender is a dial-up is incorporated into the overall Intercept Anti-Spam decision.*

10. You can customize the Reputation Enabled Defense **Reject Message**.

    Use “%s” to specify the IP address of the rejected sender.

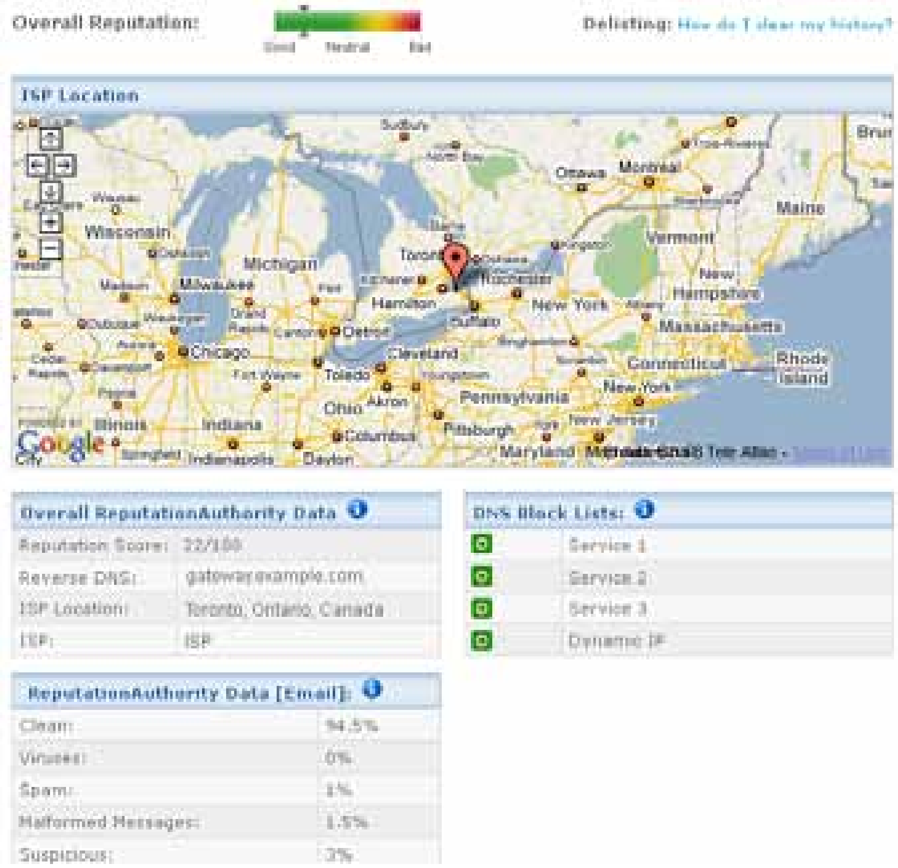
    For example,

    ```
    go to http://www.reputationauthority.org/lookup?ip=%s
    ```

Reputation Enabled Defense rejection, infection, and dial-up log messages include a URL similar to this example:

```
450: blocked by Intercept:
http://www.reputationauthority.org/lookup?ip=207.236.65.226&d=4ECD2A71BB0D0E6A&u=45F00D38BFC08
```

where the IP address is the connecting server that was rejected. The “d=” and “u=” section are domain and user hashes for the domain and sender reputation. Click the URL to open up the Reputation Enabled Defense (powered by ReputationAuthority) web page that displays reputation statistics for the specified IP address, domain, and user.



Overall ReputationAuthority Data

Reputation Score:	22/100
Reverse DNS:	gatewayexample.com
ISP Location:	Toronto, Ontario, Canada
ISP:	ISP

DNS Block Lists:

✓	Service 1
✓	Service 2
✓	Service 3
✓	Dynamic IP

ReputationAuthority Data [Email]:

Clean:	94.5%
Viruses:	0%
Spam:	1%
Malformed Messages:	1.5%
Suspicious:	3%

11. To check incoming messages against the spam information gathered by the RED network, select the **Enable Reputation Enabled Defense for Anti-Spam** check box.
12. In the **Check Relays** text box, specify how many received headers to check with RED.

For example, an email message may have been relayed by four mail servers before it reached the XCS. Use this field to specify how many relay points, starting from the latest headers to the earliest, should have their reputation checked by RED. Acceptable values are between “0” and “ALL”. The default is “0”.

> **Note** *You must enable Check Relays if the system is installed behind another MTA or mail gateway. This action makes sure that the relay before the intermediary MTA is checked.*

13. In the **Exclude Relays** field, specify how many received headers to exclude from RED checks, starting from the earliest header to the most recent.

    For example, if **Check Relays** is enabled, setting this value to “1” means that the first relay point is not checked. Note that some ISPs include the originating dial-up IP as the first relay point which can lead to legitimate mail being classified as spam by RED. We recommend you set this value to “0” (off) or “1”. The default is “0”.

    > ***Note*** *The Exclude Relays setting is only enabled if you enable Check Relays.*

    As an example of using the **Check Relays** and **Exclude Relays** options, consider this scenario:

    ```
    Server A -> Server B -> Server C -> Server D -> WatchGuard XCS
    ```

    With the mail relayed through four previous servers (A-D), the received headers of a message appear in this order:

    ```
    Received: DReceived: CReceived: BReceived: A
    ```

    With **Check Relays** enabled, the XCS starts with server D and checks the configured number of received headers. If **Check Relays** is set to “3”, it checks D, C, and B.

    Use the **Exclude Relays** option to ignore the configured number of received headers starting at the end of the header list regardless of what the **Check Relays** option is set to. If **Exclude Relays** is set to “1”, then server A is excluded from the checks.

14. Click **Apply**.

Token Analysis

Token Analysis is a sophisticated method of identifying spam based on statistical analysis of mail content. Simple text matches can lead to false positives because a word or phrase can have many meanings depending on the context. Token Analysis provides a way to accurately measure how likely any particular message is to be spam without having to specify every word and phrase.

Token Analysis derives a measure of a word or phrase contributing to the likelihood of a message being spam. This is based on the relative frequency of words and phrases in a large number of spam messages. From this analysis, it creates a table of tokens (words associated with spam) and associated measures of how likely a message is spam.

Token Analysis analyzes a new message, extracts the tokens (words and phrases), finds their measures from the table, and aggregates these measures to produce a spam metric for the message. This spam metric is the score assigned by Token Analysis to use in the Intercept Anti-Spam decision.

Token Analysis has a built-in weighting mechanism that assigns a value between 0 and 100 to indicate whether a message is spam. A message with a low metric (closer to 0) is considered to be legitimate, while a message with a high metric (closer to 100) is considered to be spam. Token Analysis uses three sources of data to build its run-time database:

- The initial default database based on analysis of known spam.
- Tables derived from an analysis of local legitimate mail. This is referred to as “training”.
- Training provided by spam from Pattern Filter Spam, Reputation, Brightmail, DNSBL, UBL, SPF, and DomainKeys Intercept components.

How Token Analysis Works

Consider this simple message:

```
---------------------------------------------------------------
Subject: Get rich quick!!!!
Click on http://getrichquick.com to earn millions!!!!!
---------------------------------------------------------------
```

Token Analysis breaks the message down into these tokens:

```
[Get] [rich] [quick!!!] [Click] [on] [http://getrichquick.com] [to] [earn]
[millions!!!!!]
```

Each token is looked up in the database and a spam metric is retrieved. The token "Click" has a high metric of 91, whereas the word "to" is neutral (indicating neither spam nor legitimate.) These metrics are aggregated using statistical methods to give the overall score for the message of 98.

Mail messages with a spam metric of 90 or greater are very likely to be spam. Lower values (50-60) indicate possible spam, while very low values (20-25) are unlikely to be spam. These spam metrics are the score assigned by Token Analysis as part of the final Intercept Anti-Spam decision.

Token Analysis Training

When first enabled, the WatchGuard XCS immediately starts training on inbound and outbound mail. The WatchGuard XCS uses the Token Analysis Anti-Spam feature for spam and legitimate mail training.

Token Analysis training includes:

- The initial default database based on analysis of historical known spam
- Training derived from analysis of local legitimate mail (trusted outbound mail)
- Spam training provided through mail processed by the Intercept Anti-Spam features

Local outbound mail is assumed to be trusted and not spam, and the frequency of the words found in these messages can be used to modify the values supplied by WatchGuard's default training database. For example, a mortgage company uses the word "refinance" frequently in its regular mail. The likelihood of this word suggesting spam is therefore reduced.

Token Analysis trains messages from these sources as legitimate mail:

- Specific Access Pattern Trust
- Reputation Whitelist (Reputation Enabled Defense list of hosts that are known to send legitimate mail)
- Pattern Filter train action
- User submitted legitimate mail (Not Spam)
- Trusted Subnet (mail originating on a specific trusted network interface)

Token Analysis trains messages for spam if one of these features classifies a message as spam:

- Reputation Enabled Defense
- DNS Block Lists
- URL Block Lists
- Pattern Filter spam

- Backscatter Detection
- Domain Keys and SPF
- Brightmail
- User submitted Spam

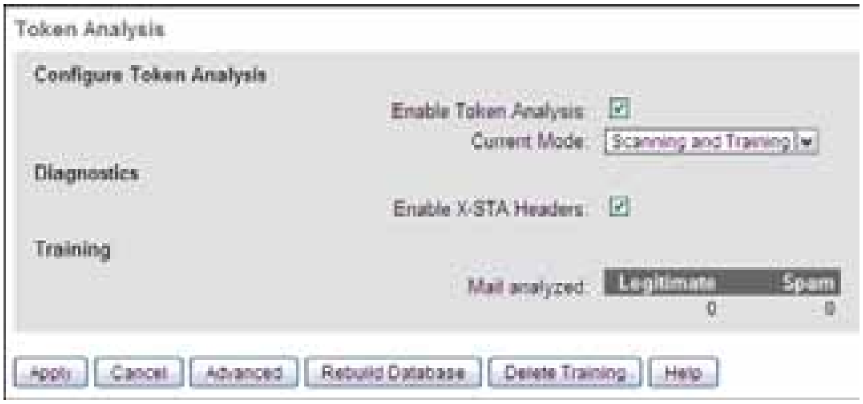
Training Period

Depending on the amount of mail sent and received in your environment, it can take several days of mail processing and training to properly adjust the default training database for the content of your organization's mail flow. At least 500 legitimate mail messages and 1000 spam messages must be processed to accurately train the WatchGuard XCS.

Configure Token Analysis

To configure Token Analysis

1. Select **Security > Anti-Spam > Anti-Spam**.
2. Select **Token Analysis**.



Token Analysis

Configure Token Analysis

Enable Token Analysis: ☑

Current Mode: Scanning and Training

Diagnostics

Enable X-STA Headers: ☑

Training

Mail analyzed:

Legitimate	Spam
0	0

3. Select **Enable Token Analysis**.
4. From the **Current Mode** drop-down list, select a Token Analysis mode.
    - **Training Only** – Token Analysis analyzes and trains on local mail, but the results of the scan do not contribute to the overall Intercept message score.
    - **Scanning and Training** – Token Analysis analyzes and trains on local mail. The results of the scan contribute to the overall Intercept message score.
5. Click **Apply**.

Database and Training

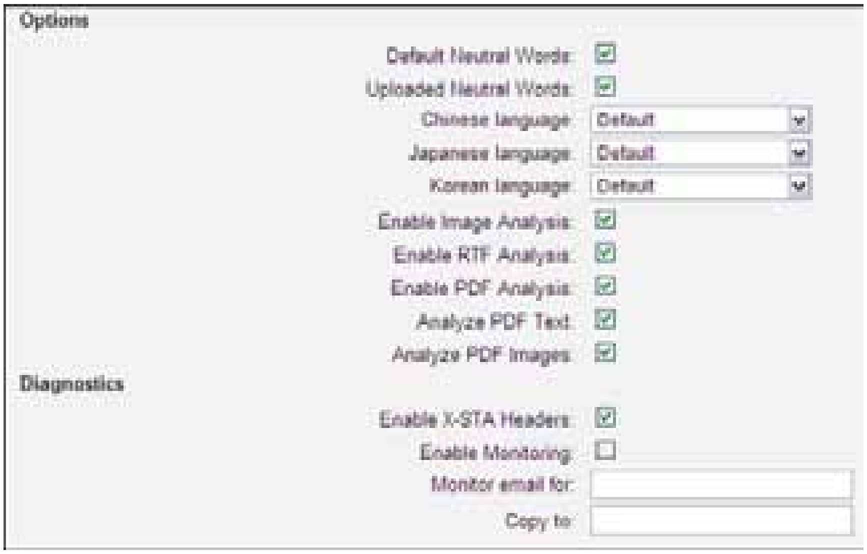
The Token Analysis database is built and rebuilt at two hour intervals from several sources, for example, the supplied spam data, updated data from WatchGuard, trained spam from other Intercept features, and local training. The database is not built for the first time until two hours after installation, and you can click **Rebuild Database** at any time to rebuild the Token Analysis database.

You must delete all training material if your system has been misconfigured and starts to treat trusted mail as untrusted or vice versa. Click **Delete Training** to remove all training material.

Token Analysis Advanced Options

To configure advanced Token Analysis options, click **Advanced**.

> ***Note*** *These options are for advanced configuration only, and we recommend that you use the default values. Modifications to the default values can decrease Token Analysis accuracy and should be used with care.*



Options

Default Neutral Words: ☑
Uploaded Neutral Words: ☑
Chinese language: Default
Japanese language: Default
Korean language: Default
Enable Image Analysis: ☑
Enable RTF Analysis: ☑
Enable PDF Analysis: ☑
Analyze PDF Text: ☑
Analyze PDF Images: ☑

Diagnostics

Enable X-STA Headers: ☑
Enable Monitoring: □
Monitor email for:
Copy to:

Neutral Words

Neutral words are words that may or may not indicate spam. For example, a mortgage company may want to build a neutral word list that includes “refinance” or “mortgage” because these words show up quite frequently in spam mail. By adding them to the neutral word list, the likelihood of this word suggesting spam would be reduced to a neutral value.

- **Default Neutral Words** – Select the check box to enable the WatchGuard neutral words list. This list helps prevent pollution of the Token Analysis database. We recommend that you leave this option enabled.
- **Uploaded Neutral Words** – Select the check box to enable the uploaded neutral words list.

To upload a file, click **Upload Neutral Words**. The file must be in text format and contain a list of neutral words with one word per line. If you upload a new list, it replaces the previous neutral words list.

> ***Note*** *The WatchGuard XCS automatically rebuilds the Token Analysis database during the upload of a neutral words list.*

Token Analysis and Languages

The Token Analysis spam database is based on English language spam. As a result, it may not be initially responsive to spam created in other languages. The ability to learn means that it can readily adapt to other languages. Token Analysis trains on local legitimate mail from the moment the system is started. This helps properly characterize the local language use by building up a database of good words to help prevent mail messages from being classified as spam. To train the system with known local language spam mail, we recommend that you set up rules to use the *Certainly Spam* action in the Pattern Filters. Messages specified as spam are forwarded to Token Analysis and increase its database of local language words.

Japanese, Chinese, and Korean Languages

The language options alter the Token Analysis processing behavior for Japanese, Chinese, and Korean language messages to make sure they are not automatically classified as spam. These include these character sets:

- **Japanese major character sets** – ISO-2022-JP, EUC-JP, Shift-JIS
- **Chinese major character sets** – GB2312, HZ-GB-2312, BIG5, GB7589, GB7590, GB8565.2-88, GB12052, GB/T12345, GB/T13131, GB/T13132, GB/T13000.1, ISO-2022-CN, ISO-2022-CN-EXT
- **Korean major character sets** – KS C 5601 (KS C 5601-1987), EUC-KR, ISO-2022-KR

For each character set, select how Token Analysis processes the message:

- **Default** – All content is processed by Token Analysis. If you receive legitimate mail in these languages, this may result in false positives.
- **No Token Analysis Scan** – Token Analysis scanning is turned off for all messages containing Japanese, Chinese, and Korean language characters.
- **Lenient Token Analysis Scan** – Token Analysis scanning is turned off for only the parts of the message containing Japanese, Chinese, and Korean language characters. The rest of the message is processed normally. If there are 20 or fewer tokens in the message of non-Japanese, Chinese, and Korean characters, the Token Analysis scan is skipped for that message.

Image Analysis

An image spam email message typically consists of random text or no text body and contains an attachment picture (usually .gif or .jpg format) that supplies the text and graphics of the spam message. These types of spam messages are difficult to detect because the message contains no helpful text or URL characteristics that can be scanned and analyzed. The Image Spam Analysis feature performs advanced analysis of image attachments to help determine if the message is spam or legitimate mail. Similar to the other Anti-Spam features that detect spam characteristics in the text of a message, the Image Analysis feature extracts certain characteristics of the attached image to determine if these characteristics are similar to those seen in actual spam messages.

1. Make sure the **Enable Token Analysis** option is enabled using **Scanning and Training** mode.
2. Select the **Enable Image Analysis** check box in the **Options** section.
3. Click **Apply**.

Allow at least 24 hours for the Token Analysis scanner to scan and train incoming mail and update its database to see an improvement in spam catch rates. To accelerate this process:

1. Select **Administration > Software Updates > Security Connection**.
2. To retrieve the latest Token Analysis database updates, click **Connect Now**.
3. Select **Security > Anti-Spam > Anti-Spam > Token Analysis**.
4. Click **Rebuild Database** to perform a manual rebuild of the Token Analysis database.
   The database is rebuilt automatically every two hours.

RTF Analysis

Spammers can embed spam text and images in RTF (Rich Text Format) documents. The Token Analysis scanner creates tokens for unique RTF properties to be able to detect characteristics of RTF spam.

PDF Spam Analysis

In response to the effectiveness of image spam detection technologies, spammers have attempted to circumvent the anti-spam scanners by embedding spam text and images in PDF (Portable Document Format) documents. Within these PDF documents, the images and text themselves can be further obfuscated with various image distortion techniques and using “word salad” text that contains valid text included with the spam message text. A further technique used to avoid detection is to compress the PDF into an archive file, for example, .zip. Token Analysis can improve detection of PDF spam by analyzing specific information in the PDF, for example, the document meta-properties (author, creation date, etc.) and the text and images contained in the PDF. The Token Analysis scanner creates tokens for each of these unique PDF properties to be able to detect characteristics of PDF spam.

> ***Note*** *The PDF Analysis feature uses the Token Analysis component to analyze PDF spam messages. You must enable Token Analysis for PDF Spam detection to work. To perform content inspection of archive files, for example, .zip, that contain PDF files, you must enable Kaspersky Anti-Virus.*

Tokens generated by the PDF analysis feature (by analyzing text in the PDF) are also utilized by the Spam Words and URL Block List (UBL) features. They cannot be used for the Objectionable Content Filter.

- **Enable PDF Analysis** – Enables PDF analysis to allow the system to scan PDF files for spam. This is enabled by default.

> ***Note*** *If the PDF document size is larger than 45kb, analysis of the document is skipped. Larger documents are less likely to be spam messages.*

- **Analyze PDF Text** – Select this check box to extract and analyze the text in a PDF file. This allows the scanner to examine the PDF text for words that may indicate it is a spam message. Tokens created from the text in a PDF are used by Token Analysis, Spam Words, and the URL Block list features.
- **Analyze PDF Images** – Select this check box to analyze images in PDF documents for image spam. You must also enable the **Image Analysis** option to analyze images in PDF documents.

> ***Note*** *PDF text and image analysis are enabled by default. Disable these options if there is an increased amount of false positives (legitimate mail identified as spam), or if system message processing performance is affected.*

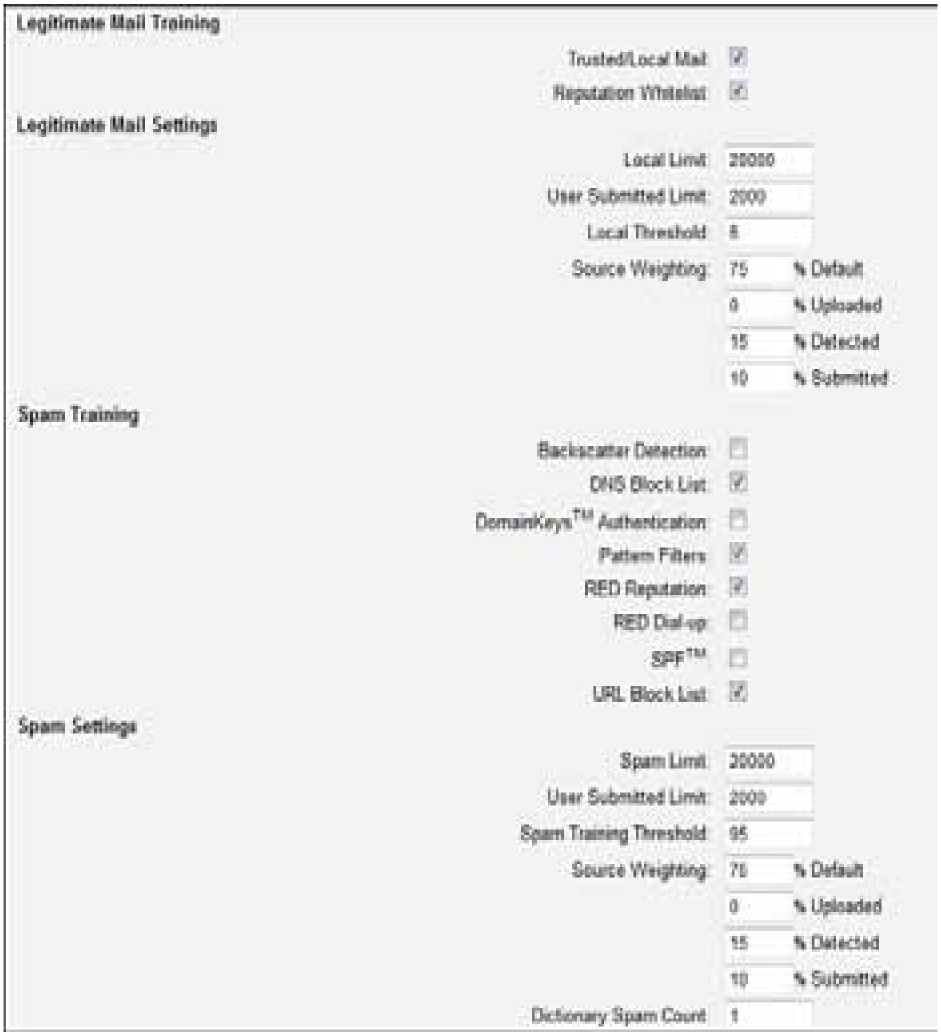
Diagnostics

The diagnostics section allows you to configure diagnostic options for Token Analysis to help with troubleshooting.

- **Enable X-STA Headers** – This setting inserts X-STA (Token Analysis) headers into all messages. These headers are not visible to the user (although you can filter them in most mail clients), but you can use them to gather information on why mail is processed in a particular way.

  These headers are inserted:

  - **X-STA-Metric** – The score assigned by Token Analysis, for example, 95, which indicates a spam message.
  - **X-STA-NotSpam** – Indicates the words with the highest non-spam value found in the message.
  - **X-STA-Spam** – Indicates the words with the highest spam value found in the message.
- **Enable Monitoring** – Select the check box to monitor messages received by the specified email address.
- **Monitor email for** – Type an email address that you want to monitor.
- **Copy to** – Copy messages and the Token Analysis diagnostic to this email address.



Legitimate Mail Training

Trusted/Local Mail ☑

Reputation Whitelist ☑

Legitimate Mail Settings

Local Limit: 20000

User Submitted Limit: 2000

Local Threshold: 5

Source Weighting: 75 % Default

0 % Uploaded

15 % Detected

10 % Submitted

Spam Training

Backscatter Detection ☐

DNS Block List ☑

DomainKeys™ Authentication ☐

Pattern Filters ☑

RED Reputation ☑

RED Dial-up ☐

SPF™ ☐

URL Block List ☑

Spam Settings

Spam Limit: 20000

User Submitted Limit: 2000

Spam Training Threshold: 95

Source Weighting: 75 % Default

0 % Uploaded

15 % Detected

10 % Submitted

Dictionary Spam Count: 1

Legitimate Mail Training

Local mail is assumed to be not spam, and Token Analysis can train local mail to identify tokens that indicate legitimate mail.

- **Trusted/Local Mail** – To train all local trusted network mail for Token Analysis, select the **Trusted/Local Mail** check box. This includes outbound mail from a trusted subnet (based on the network interface with the **Trusted Subnet** option enabled), and mail trusted by a Pattern Filter.

> ***Note*** *If you do not train on local trusted mail, use the Heuristic 1 Intercept Decision strategy to de-emphasize Token Analysis. This prevents false positives when you use the Heuristic 2 strategy.*

- **Reputation Whitelist** – To train on legitimate mail based on Reputation Enabled Defense whitelists of hosts that are known to send legitimate mail, select the **Reputation Whitelist** check box.

  Reputation Whitelists are similar to block lists that are used to identify servers that send a lot of spam messages. Whitelists indicate messages that originate from a server IP address that never sends spam. This information is very useful in the overall Anti-Spam decision. For example, in certain cases, a message can receive a high Token Analysis score, but because the server is listed on a whitelist, this indicates the message is most likely legitimate mail. This feature also provides a method to train the Token Analysis feature for mail environments that do not process the local outbound mail flow.

Legitimate Mail Settings

- **Local Limit** – Type the maximum number of messages from local users to use for Token Analysis training. When the limit is reached, older training messages are deleted as new messages arrive. Default is 20000.
- **User Submitted Limit** - Type the maximum number of user submitted legitimate mail messages used for training. When the limit is reached, older messages are deleted as new messages arrive. The default is 2000. You can enter values between 200 and 100000.
- **Local Threshold** – Set the threshold for messages from local users to be used for training. If the Token Analysis classification for the message is greater than or equal to the specified number, the message is used for training.
- **Source Weighting %** – For Token Analysis to be useful and efficient, the training must be based on well selected data. The initial database supplied by WatchGuard represents well selected data, and is therefore highly weighted, compared to uploaded legitimate mail or legitimate mail from the trusted network.
  - **Default** – Type a percentage for the weight of the WatchGuard maintained Token Analysis database of valid mail.
  - **Uploaded** – Type the weight of locally uploaded valid mail. To upload legitimate mail, click **Upload Legitimate Mail**. The mail must be in plain-text Unix mbox format. You must upload a minimum of ten messages to be effective.
  - **Detected** – Enter the weight of mail detected from trusted networks that are automatically trained as valid mail.
  - **Submitted**– Weight of legitimate mail messages submitted by end users.

> ***Note*** *When you upload mail, we recommend that you set the weighting to 60% for Default, 20% for Upload, 10% for Detected, and 10% for Submitted. Significant changes to the source weighting can decrease Token Analysis accuracy.*

Spam Training

Select which features are used for spam training:

- **Backscatter Detection** – Train mail marked as spam by Backscatter Detection.
- **DNS Block List** – Train mail marked as spam by DNS Block Lists.
- **DomainKeys Authentication** – Train mail marked as spam by DomainKeys.
- **Pattern Based Message Filtering** – Train mail marked as spam by Pattern Filters.
- **RED Reputation** – Train mail marked as spam by Reputation Enabled Defense.
- **RED Dial-up** – Train mail marked as spam by Reputation Enabled Defense DUL (dial-up).
- **SPF** – Train mail marked as spam by SPF.
- **URL Block List** – Train mail marked as spam by the URL Block Lists.

Spam Settings

- **Spam Limit** – Type the maximum number of spam messages used for training.
- **User Submitted Limit** - Type the maximum number of user submitted spam messages used for training. When the limit is reached, older messages are deleted as new messages arrive. The default is 2000. You can enter values between 200 and 100000.
- **Spam Training Threshold** – Set the threshold for spam messages to use for training.
  If the Token Analysis classification for the message is less than or equal to the specified number, use the message for training.
- **Source Weighting** – For Token Analysis to be useful and efficient, the training must be based on well selected data. The default database supplied by WatchGuard represents well selected data and is therefore highly weighted, compared to uploaded spam mail.
  - **Default** – Type a percentage for the weight of the WatchGuard maintained Token Analysis database of spam mail.
  - **Uploaded** – Type the weight of locally uploaded spam mail. To upload spam mail, click **Upload Spam Mail**. The mail must be in plain-text Unix mbox format. Upload a minimum of ten messages to be effective.
  - **Detected** – Weight of mail from DNSBL, UBL Block Lists, Pattern Filters or Reputation Enabled Defense automatically trained as spam.
  - **Submitted**– Weight of spam messages submitted by end users.

> ***Note*** *When you upload mail, we recommend that you set the weighting to 60% for Default, 20% for Upload, 10% for Detected, and 10% for Submitted. Significant changes to the source weighting can decrease Token Analysis accuracy.*

Dictionary Spam Count

Recent changes to the way that spammers compose their messages can reduce the effectiveness of the Token Analysis filter. By introducing large numbers of normal words into their spam messages, spammers can hide their content because the normal words outweigh the spam words and result in a low spam count. More aggressive settings can result in more false positives. The WatchGuard XCS counters this in two ways:

1. All words in the dictionary are assigned a base level of how likely they are to be spam. In a normal message, this increased level does not result in a false positive, since the overall count is low. In a spam message, the result is different; the normal words do not counteract the spam content, and the message is correctly identified as spam.
2. Training on local mail now works to reduce this base level closer to zero. This further reduces the likelihood of a false positive.

The **Dictionary Count** is set to “1” by default. This should be sufficient for most situations. We recommend that you only change the default value if these conditions occur:

- If there are too many false positives and this is not alleviated by training, then the **Dictionary Count** should be set to “0” to disable this feature.
- If too much spam is getting through, then increase the **Dictionary Count**. Increase the value to “10”. If this results in too many false positives, reduce it to “5”.

> ***Note*** *Only modify the dictionary count setting if other measures (training, threshold changes, uploading spam and/or legitimate mail) have been tried and have not provided the desired result.*

Troubleshoot Token Analysis

Token Analysis is a very effective anti-spam tool and provides the mail administrator with a variety of options to finely tune this feature for their particular environment. With these advanced controls, there is a greater chance of creating a configuration that may result in excessive false positives (mail marked as spam when they are legitimate) or false negatives (mail not marked as spam when they are spam.)

These are some considerations when troubleshooting issues with Token Analysis:

For excessive false positives:

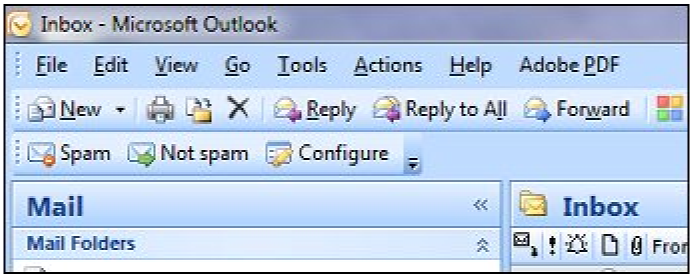
- Make sure that the system has gone through a cycle of training.
- Make sure that any mailing lists that the organization sends out are trusted (with Pattern Filters) as **Accept**.
- Check for tokens that may be words used by the organization for their regular business. For example, a financing company would want the words “mortgage” or “refinance” to be allowed as legitimate tokens.
- Lower the component weighting in the Intercept settings.

For excessive false negatives:

- Check that any mailing lists received by the users are trusted with Pattern Filters as **Bypass** or **Accept**.

WatchGuard XCS Outlook Add-in

The WatchGuard XCS Outlook Add-in places special **Spam** and **Not Spam** buttons on your Microsoft Outlook client toolbar. This tool allows you to report any spam messages that bypassed the spam filters and were delivered to your inbox, and also report false positives where legitimate messages were classified as spam.


Inbox - Microsoft Outlook
File Edit View Go Tools Actions Help Adobe PDF
New Reply Reply to All Forward
Spam Not spam Configure
Mail
Mail Folders
Inbox
From

To report and train on spam messages that appear in your inbox, you can select the message, then click "Spam". To report and train on legitimate messages that were classified as spam, select the message, then click "Not Spam".

When you click the **Spam** button:

- The message can remain in the inbox, be moved to the Junk folder, or deleted.
- The message is trained as spam by the WatchGuard XCS.
- The message is relayed to WatchGuard servers for training.
- The sender is added to your personal Blocked Senders List.

When you click the **Not Spam** button:

- The message is trained as legitimate mail (Not Spam) by the WatchGuard XCS.
- The message is relayed to WatchGuard servers as legitimate mail training.
- The sender is added to your personal Trusted Senders List.

See *Custom Actions for Pattern Filters and Content Rules* to configure User Reported Spam and Not Spam training options on the Custom Actions page.

> ***Note*** *The ability to configure WatchGuard XCS Outlook Add-in training options and end user Trusted/Blocked Senders List settings requires WatchGuard XCS 9.1 Update 2 or greater. For earlier versions of XCS, the messages are relayed to WatchGuard only, and you must manually create a Pattern Filter to not train on outbound messages sent to @mailsupport.watchguard.com.*

Download and Install the WatchGuard XCS Outlook Add-in

The WatchGuard XCS Outlook Add-in is available for these versions of Outlook:

- Outlook 2003
- Outlook 2007

To download the Add-in for your version of Outlook:

1. Select **Support > Microsoft Outlook Add-ins** from the WatchGuard XCS Web UI.
   The WatchGuard Support Center appears.
2. From the WatchGuard Support Center, select **Download Software**.
3. Select **WatchGuard XCS**.
4. Select the download link for the Add-in for your version of Outlook.

Operating System and Language Support

The WatchGuard XCS Outlook Add-in supports these operating systems and languages:

- Windows XP
- Windows Vista
- Windows 7

Supported languages:

- English (default)
- French (fr)
- Spanish (es)
- Japanese (ja)
- Simplified Chinese (zh-CHS)

Software Requirements

The WatchGuard XCS Outlook Add-in requires the following client software:

- .NET Framework 3.5 or greater (Not included with the Outlook Add-in .zip file. You must download the latest .NET Framework software from Microsoft.)
- Windows Installer 3.1
- Microsoft Office Primary Interop Assemblies (PIA)
- Visual Studio Tools for Office (VSTO)

Use the *setup.exe* file to install the WatchGuard XCS Outlook Add-in and prerequisites (except the .NET Framework software which must be installed separately).

If you already have the prerequisite software installed, you can install the WatchGuard XCS Outlook Add-in with the *XCSOutlook2003AddinInstaller.msi* or *XCSOutlook2007AddinInstaller.msi* file. Network administrators can use the *.msi* installation file to push the add-in to desktop workstations in an Active Directory domain, but the prerequisite software must already be installed on the desktop workstations or be pushed by the administrator before the add-in installation.

Install the WatchGuard XCS Outlook Add-in

To install the WatchGuard XCS Outlook Add-in:

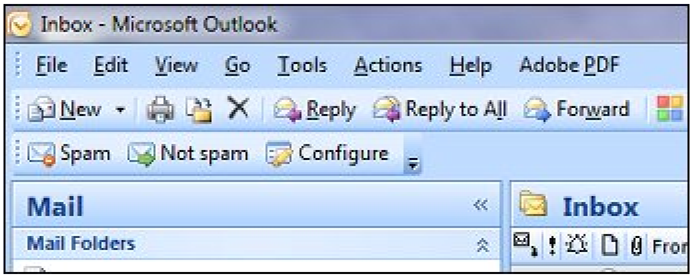
1. Close Microsoft Outlook if it is currently running.
2. Make sure you have downloaded and installed the .NET Framework (3.5 or greater) software.
3. Unzip the download package.
4. Double-click the *setup.exe* installation file.

   You are prompted to install each prerequisite software as required.
5. Follow the prompts to continue the installation for each prerequisite.
6. Follow the prompts to install the WatchGuard XCS Outlook Add-in.
7. Click **Close** when the installation completes.

Configure the WatchGuard XCS Outlook Add-in

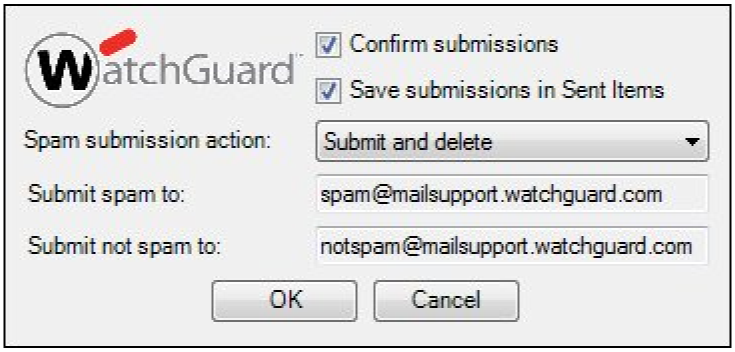
To configure the WatchGuard XCS Outlook Add-in:

1. Start Microsoft Outlook.
   *A new toolbar appears that displays the **Spam**, **Not Spam**, and **Configure** buttons.*


Inbox - Microsoft Outlook
File Edit View Go Tools Actions Help Adobe PDF
New Reply Reply to All Forward
Spam Not spam Configure
Mail
Mail Folders
Inbox
From

> ***Note*** *You may be prompted to confirm the installation of the Outlook Add-in when Microsoft Outlook starts.*

2. Click **Configure**.



☑ Confirm submissions

☑ Save submissions in Sent Items

Spam submission action: Submit and delete

Submit spam to: spam@mailsupport.watchguard.com

Submit not spam to: notspam@mailsupport.watchguard.com

3. To ask for confirmation when you click the **Spam** or **Not Spam** button, select the **Confirm submissions** check box.
4. To save any messages that you submit as Spam or Not Spam in your Sent Items folder, select the **Save submissions in Sent Items** check box.
5. From the **Spam submission action** drop-down list, select the action to perform on a spam message when you click the Spam button:

   - **Submit** – Submits the spam message. The message remains in the inbox.
   - **Submit and delete** – Submits the spam message and then deletes the message.
   - **Submit and move to Junk folder** – Submits the spam message and moves the message to the Junk folder.

6. The **Submit spam to** text box displays the email address to which to send "Spam" message submissions.
   The default is spam@mailsupport.watchguard.com.

   The **Submit not spam to** text box, displays the email address to which to send "Not Spam" message submissions.
   The default is notspam@mailsupport.watchguard.com.

7. Click **OK**.

Backscatter Detection

Backscatter is a type of spam attack where spam mail is sent to email servers with forged header information for the Envelope Sender address. If the email server bounces this email back to the sender, a bounced message usually has the Envelope Recipient set to the Envelope Sender of the original message, and the undeliverable message notification is sent to the email address of the innocent user. There can also be other unsuspecting email servers in the message path, and in a large spam campaign the target systems are flooded with these backscatter spam messages.

Backscatter spam is mitigated with special signing techniques, for example, Bounce Address Tag Validation (BATV). BATV uses message signing to sign the local Envelope Sender address. If the message is bounced back, the Envelope Recipient address signature is validated which prevents any undeliverable message bounce notifications from being returned to a forged address.

> ***Note*** *Messages are not signed if they are sent to a local internal recipient.*

For example, if the WatchGuard XCS sends an outgoing message to an external user from: user@example.com, a PRVS (Simple Private Signature) tag is created utilizing the key index, the timestamp and expiration term of the message, and a private key. An SHA1 message digest is generated for this information that results in this format:

```
<prvs=[Key Index][Expiry][Digest][Email address]>
```

With this information:

```
Key Index = 0Expiry = 110 (generated from the current time and the expiry time)SHA
1 digest = 450a98Email Address = user@example.com
```

Results in the email address are rewritten with this PRVS tag:

```
<prvs=0110450a98=user@example.com>
```

If this message is bounced back to the WatchGuard XCS, it extracts and verifies the address signature. If the signature cannot be verified, or if it is invalid or expired, the WatchGuard XCS can reject the message immediately, or contribute to the overall Intercept Anti-Spam score for the message.

> ***Warning*** *Verify that the gateway device, for example, the WatchGuard XCS, is the only device performing PRVS tag signing and verification, and that you disable PRVS tag signing and verification on any internal mail servers.*

Intercept Anti-Spam Processing

For Intercept Anti-Spam processing, the Backscatter Detection feature creates a result code between 0 and 100 for the message. This table describes the result codes that are returned for a message after Backscatter Detection processing.

Any result greater than code 50 results in the message being considered spam, and the configured Backscatter Detection Intercept weight is applied to the overall Intercept Anti-Spam score for the message.

Code	Description
0	No PRVS checking or signing was performed
1	OK (signature verified)
50	Unsigned
51	Invalid key
52	Invalid signature
53	Signature expired
60	Syntax error 1
61	Syntax error 2
62	Syntax error 3

Anti-Spam Header

Any Backscatter Detection results are added to the Anti-Spam header (if enabled), using this format:

```
<Backscatter on/off><Explanation/Result Code>
```

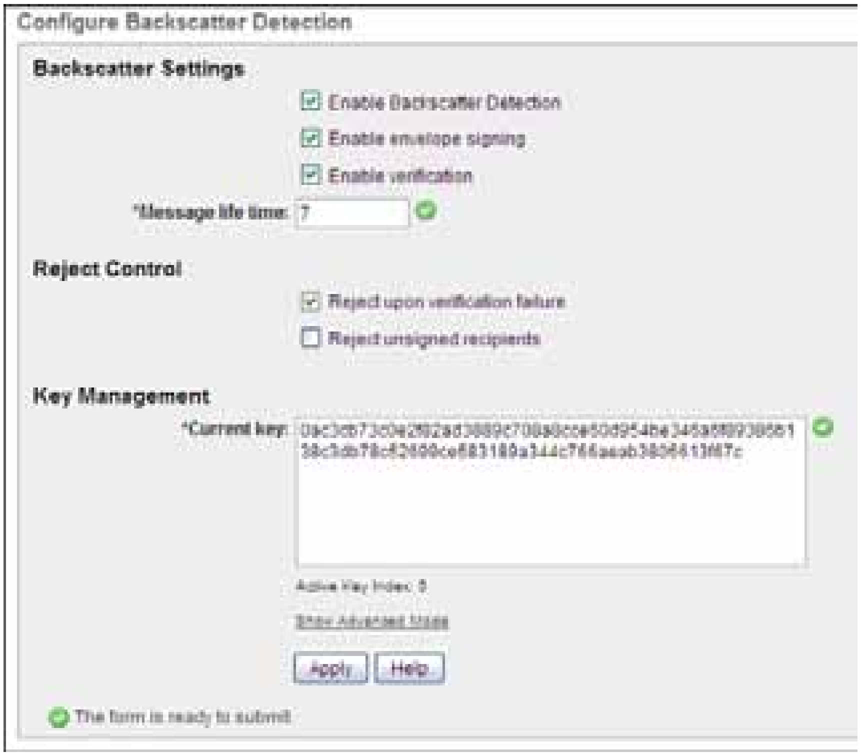
For example:

```
bsctr:off
bsctr:spam/52
bsctr:passed/1
```

Configure Backscatter Detection

To enable and configure Backscatter Detection:

1. Select **Security > Anti-Spam > Anti-Spam**.
2. Select **Backscatter Detection**.
   The Configure Backscatter Detection page appears.



Configure Backscatter Detection

Backscatter Settings

☑ Enable Backscatter Detection

☑ Enable envelope signing

☑ Enable verification

*Message life time: 7

Reject Control

☑ Reject upon verification failure

□ Reject unsigned recipients

Key Management

*Current key: 0ac3db73c0e2f82ad3889c708a8cce50d954be345a88938681 38c5db78c62680ce583189a344c766aeab38066136f7c

Active Key Index: 5

Show Advanced Mode

The form is ready to submit

3. Select the **Enable Backscatter Detection** check box.

> ***Note*** *If you enable Backscatter Detection and disable envelope signing and verification, the XCS strips the PRVS tags (even if invalid) from the message and delivers the message to its destination.*

4. To sign outgoing (non-local) email messages with the Backscatter verification signature, select the **Enable envelope signing** check box.
5. To verify the sender address signature of incoming messages, select the **Enable Verification** check box.

   This option makes sure that invalid addresses are rejected immediately or scanned by Intercept Anti-Spam depending on your configuration.
6. In the **Message life time** text box, type the number of days before the signature expires and is considered invalid.

   Expired signatures cause the Backscatter verification check to fail and triggers the specified action.
7. To immediately reject any messages that fail the Backscatter Detection signature validation (this includes an invalid Envelope Recipient address, syntax errors, invalid keys, and expired signature), select the **Reject upon verification failure** check box.

   When this option is disabled, the results of the Backscatter Detection scanning are used as part of the overall Intercept Anti-Spam score.
8. To reject bounce messages that do not contain any signature to verify, select the **Reject unsigned recipients** check box.

This option requires that you also enable **Reject upon verification failure**. We recommend that this option not be enabled until the XCS device has been signing and verifying message senders for a period of time to make sure that any existing unsigned messages that are still in circulation are not rejected.

9. From the **Current Key** drop-down list, select the key to use for Backscatter Detection email signing.

   The key can be up to 1024 characters. Click **Show Advanced Mode** to manually configure additional keys to use. You can also change the key in the **Current Key** text box, and the **Active Key Index** is updated automatically when you apply the settings. The previous key is saved in the advanced settings.

> ***Warning*** *You should not change the keys too frequently because any message signed with a previous key are no longer accepted and could be rejected.*
> *We recommend that you do not manually edit the keys.*

Sender Policy Framework (SPF)

Sender Policy Framework is a sender authentication technology that prevents spammers from spoofing mail headers and impersonating a legitimate email user or domain to prevent phishing attacks. Unsuspecting users can reply to these seemingly legitimate addresses with personal and confidential information.

SPF provides a means for authenticating the source of an email by sending a query to the sending domain’s DNS records. The SPF protocol allows server administrators to describe their email servers in their DNS records. By comparing the headers of the email with the SPF value, the receiving host can verify that the email is originating from the legitimate mail server for that domain. This prevents spammers from sending forged emails.

SPF actions only apply to incoming mail messages that have failed an SPF check (the email message does not match the corresponding published SPF record.) If a specific mail server does not have an existing SPF record then the message is processed normally. Administrators can misconfigure their DNS SPF records, which results in false positives and legitimate hosts being blocked from sending you mail.

The weight assigned to SPF in the Intercept settings is the score used by Intercept processing if the message fails an SPF check.

SPF is an emerging anti-fraud and anti-phishing technology that is designed primarily as a mechanism to prevent forged emails rather than an anti-spam measure. SPF is dependent on network administrators publishing their legitimate email servers in their DNS records and keeping these records current. WatchGuard recommends that customers that use SPF in their DNS infrastructure review their own SPF records to make sure they are accurate.

SPF Records

The SPF protocol allows you to describe your email servers in an SPF TXT record that is attached to the domain's DNS record. A typical SPF DNS record is:

```
example.com IN TXT "v=spf1 mx -all"
```

Add this data as a TXT record to your domain. The first part is the name part of the record, for example, “example.com”, and the text in quotes is your TXT record data.

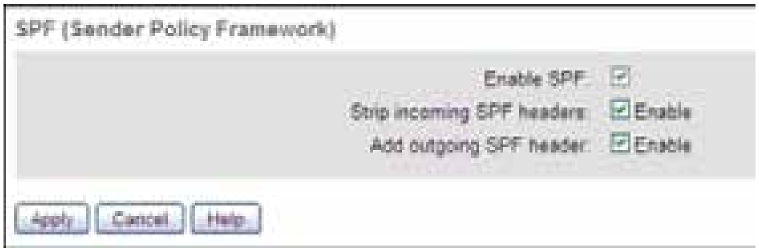
- *v=spf1* identifies the TXT record as an SPF string.
- *mx* specifies that mail can come from only the mail servers defined in your MX records.
- *-all* specifies that no other servers are able to send from the specified domain.

You can set TXT records for both domains and individual hosts.

Configure SPF

To configure SPF

1. Select **Security > Anti-Spam > Anti-Spam > SPF**.
   The SPF (Sender Policy Framework) page appears.



SPF (Sender Policy Framework)

Enable SPF: ☑
Strip incoming SPF headers: ☑ Enable
Add outgoing SPF header: ☑ Enable

2. Select the **Enable SPF** check box.
3. To strip any “Received-SPF” header from incoming messages, select the **Strip incoming SPF headers** check box.
   Spammers can attach their own forged SPF headers to create the impression that the email is from a legitimate source.
4. To add an SPF header to the outgoing message, select the **Add outgoing SPF header** check box.
5. Click **Apply**.

DomainKeys

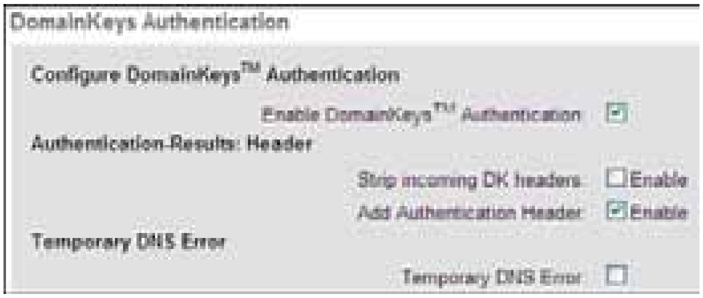
DomainKeys is a sender authentication technology that prevents spammers from spoofing mail headers and launching phishing attacks. The sender of an email message is authenticated when the XCS device queries the sending domain’s DNS records. The DomainKeys protocol allows server administrators to add a digital signature to their outgoing messages that is validated with DNS.

The domain owner generates a public and private key pair to use for signing all outgoing messages. The public key is published in their DNS records and the private key is used to sign outbound messages. By checking the signature in the headers of the email with the public key, the receiving host can verify that the email is originating from the legitimate mail server for that domain. This prevents spammers from sending forged emails. The WatchGuard XCS also supports the signing of outgoing messages with DomainKeys in Policies.

DomainKeys actions only apply to incoming mail messages that have failed a DomainKeys check (for example, an email message where the signature in the message header does not match the corresponding published DomainKeys record.) If a specific mail server does not have an existing DomainKeys record, then the message is processed normally. It is possible that administrators can misconfigure their DNS DomainKeys records, which results in false positives and legitimate hosts being blocked from sending you mail. The weight assigned to DomainKeys in the Intercept settings is the score used by Intercept processing if the message fails a DomainKeys check.

Configure DomainKeys

1. Select **Security > Anti-Spam > Anti-Spam > DomainKeys Authentication**.
   The DomainKeys Authentication page appears.



DomainKeys Authentication

Configure DomainKeys™ Authentication

Enable DomainKeys™ Authentication ☑

Authentication-Results: Header

Strip incoming DK headers □ Enable

Add Authentication Header ☑ Enable

Temporary DNS Error

Temporary DNS Error □

2. Select the **Enable DomainKeys Authentication** check box.
3. To remove *Authentication-Results:* headers attached to incoming messages, select the **Strip incoming DK headers** check box.
   This option protects against spammers who add a forged DomainKeys header to the message.
4. To add an *Authentication-Results:* header to incoming messages after they have been processed and verified by DomainKeys, select the **Add Authentication Header** check box.
5. To consider the message as spam in the event a DNS error prevents a DomainKeys lookup for a sender's key, select the **Temporary DNS Error** check box.
6. Select from these checks to consider a message as spam:

   - **No Signature When Required** – Consider the message as spam when there is no signature, even if the sender says they sign all messages.
   - **No Signature When Not Required** – Consider the message as spam when there is no signature and the sender says they may not sign all messages.
   - **Invalid Signature** – Consider the message as spam when the signature is invalid.
   - **Key Revoked** – Consider the message as spam when the key used to sign the message is no longer valid.
   - **Invalid Message Syntax** – Consider the message as spam when the signature cannot be checked because the message has invalid syntax.
   - **No Key** – Consider the message as spam when the sending domain did not provide a key for the selector specified in the message.
   - **Bad Key** – Consider the message as spam when the sending domain provides an unusable key.

   You can also perform these checks for messages from senders who test their DomainKeys implementation with a test flag inserted into their DomainKeys DNS records. We recommend that you use the default settings which perform lenient checks against these test messages.

DomainKeys Log Messages

These response codes for DomainKeys processing appear in the *Mail Log*:

```
0 - Pass
1 - Neutral
2 - Fail
3 - Soft Fail
4 - Temporary Error
5 - Permanent Error
```

The logs also indicate which DomainKeys check caused an error:

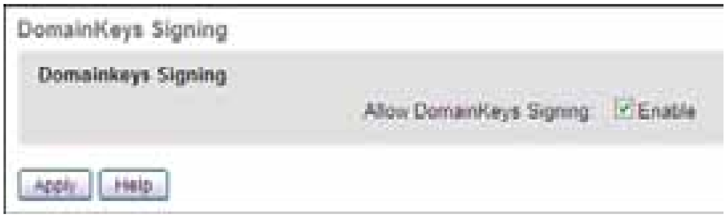
```
DomainKeys: from=user@example.com, result=permerror(bad key)
```

DomainKeys Outbound Message Signing

To enable signing of outgoing messages, you must generate a public/private key pair. The private key is used to digitally sign the message (added as a prefix to the header). The public key is published in the domain's DNS records. The receiving server can query the domain owner's DNS records for the public key and authenticate the message.

The WatchGuard XCS supports the signing of outgoing messages with DomainKeys with the Policy engine. This allows you to enable signing for only specific domains that have been configured in DNS for use with DomainKeys.

1. Select **Configuration > Mail > DomainKeys**.
   The DomainKeys Signing page appears.

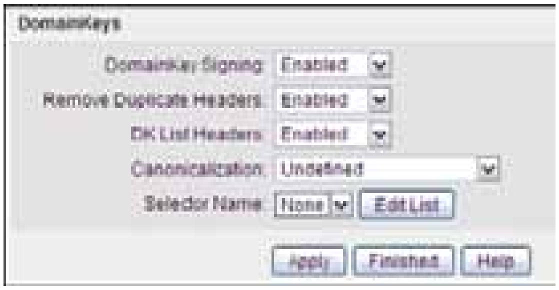


DomainKeys Signing

Domainkeys Signing

Allow DomainKeys Signing ☑ Enable

2. Select the **Allow DomainKeys Signing** check box.
3. Select **Security > Policies** > **Policies** to edit an existing policy or to add a new policy.
   The DomainKeys signing section appears in the Email tab of a policy.



DomainKeys

Domainkey Signing: Enabled

Remove Duplicate Headers: Enabled

DK List Headers: Enabled

Canonicalization: Undefined

Selector Name: None

4. Enable or disable **DomainKey Signing** for outbound messages in this policy.
5. To remove duplicate headers, for example, *Subject* and *To:* fields, from the signature calculation, select the **Remove Duplicate Headers** check box.

   Any headers listed with the “h=” tag in the DomainKeys header are filtered for duplication and the corresponding headers are removed from the message envelope. Enable this option only if you experience problems with rejected messages because of duplicate headers.

6. To add a list of the headers included into the *DomainKey-Signature:* header, select the **DK List Headers** check box.

   We recommend that you enable this option. Only the listed headers are used when verifying the signature. If this is option is disabled, then all headers after the signature are used in verifying the signature. Any headers added by intermediary servers after the message is signed invalidate the signature. Disable this option to increase security, but this can create a large number of invalid signatures because of headers added by intermediary servers.

7. From the **Canonicalization** drop-down list, specify how white space characters are treated during message signing.

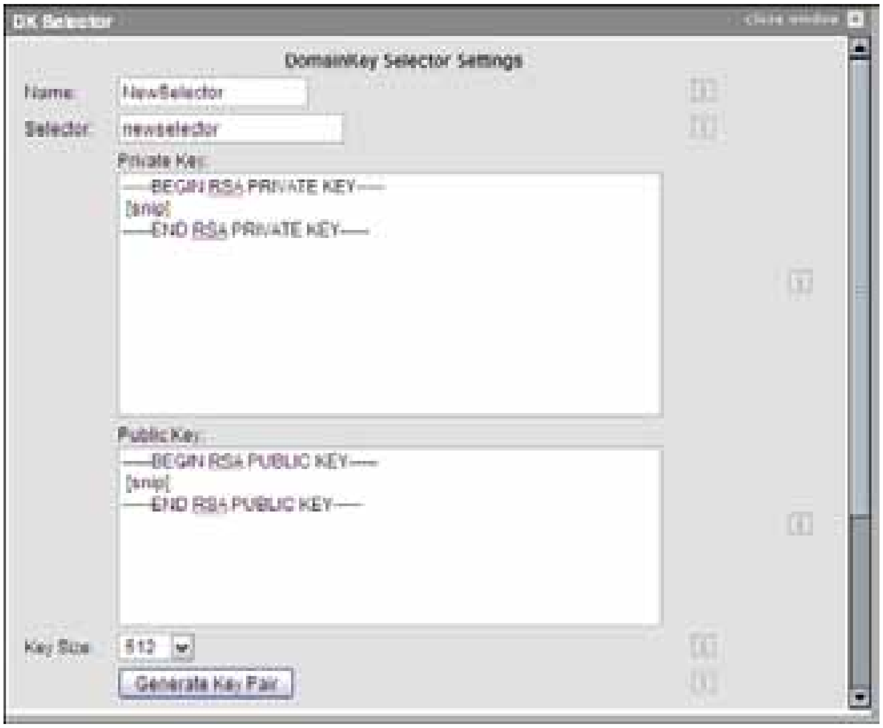
   The default is **No Folding White Space** which ignores these characters during signing. This option is more lenient so that messages reformatted in transit, for example, spaces or lines inserted into or removed from the message by intermediate servers between the signer and the receiver, are still valid. Select **Simple** to keep the signed message intact and include white space characters so that any lines that are reformatted in transit fail validation.

8. From the **Selector Name** drop-down list, choose the selector for DomainKeys signing.
9. Click **Edit List** to edit the DomainKeys Selector List.

   A DomainKeys selector is a tag for a DNS record that is used by other servers to verify your DomainKeys signature. This tag is comprised of upper and lower case letters, digits, dashes, and underscores.
   Each selector has an associated public and private key that is generated by the server by with external methods. The selector is stored in a DNS TXT record with this tag:

   ```
   <selector>._domainkey.<your_domain>
   ```

10. Click **Add Selector**.



Name: NewSelector

Selector: newselector

Private Key:

```
-----BEGIN RSA PRIVATE KEY-----
[snip]
-----END RSA PRIVATE KEY-----
```

Public Key:

```
-----BEGIN RSA PUBLIC KEY-----
[snip]
-----END RSA PUBLIC KEY-----
```

Key Size: 512

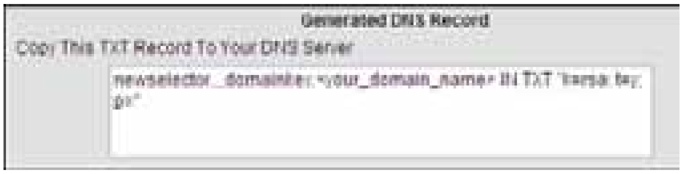
11. In the **Name** text box, type a name for this selector.
12. In the **Selector** text box, type the tag name for this selector.
13. From the **Key Size** drop-down list, select the key size for the generated key pair.

    Larger keys result in secure implementations because it decreases the probability that the keys can be compromised. We recommend that you select a minimum of 1024.

14. To generate a private/public key pair, click **Generate Key Pair**.
    The generated keys appear in the Private Key and Public Key sections.
15. To indicate that this DomainKeys DNS record is used for testing only, select the **Testing** check box.
    This allows the administrator to perform testing on the validity of their DomainKeys configuration. Receivers are generally more lenient with verification errors if the sender is in testing mode.
16. In the **Notes** text box, type any additional comments, for example, listing reasons why a particular selector is revoked.

DomainKeys DNS Record

When you create the private/public key pair, the WatchGuard XCS automatically generates a TXT record that you can sue with your DNS server for DomainKeys signing. This record contains a copy of your public key that receiving sites use to authenticate the digital signature in your outgoing messages.



Copy This TXT Record To Your DNS Server

```
newselector._domainkey.<your_domain_name> IN TXT "k=rsa; t=y;
p="
```

A domain using DomainKeys (for example, example.com) has a new subdomain in their DNS configured as "_domainkey" prefixed to the domain, for example, "_domainkey.example.com".

This is a typical DomainKeys DNS record:

```
selector._domainkey.example.com IN TXT "t=y; o=-; n=notes; r=test@example.com"
```

Administrators add this data as a TXT record to their DomainKeys domain (_domainkey.example.com). The first part is the name part of the record, and the text in quotes is entered as your TXT record data.The TXT data contains information on the DomainKeys policy.

For example,

- *o*=- means all emails from this domain are signed
- *o*=~ means some emails from this domain are signed
- *t* means Test
- *r* to enter the responsible email address
- *n* to enter free form notes on the record

Public key records are identified by a specific Selector (which allows a domain to have more than one public key in DNS) and stored in separate TXT records for that DomainKeys domain name. For example, the previously defined "_domainkey.example.com" domain contains name entries for each selector.

For example,

```
selector1
```

The corresponding TXT data consists of various options and the public key to use.

For example,

```
g=; k=rsa; t=y; p=MEwwPQRJKoZ&ldots;
```

The value after "p=" is the public key. There are also other fields available for granularity (g), test (t), and notes (n).

Brightmail Anti-Spam

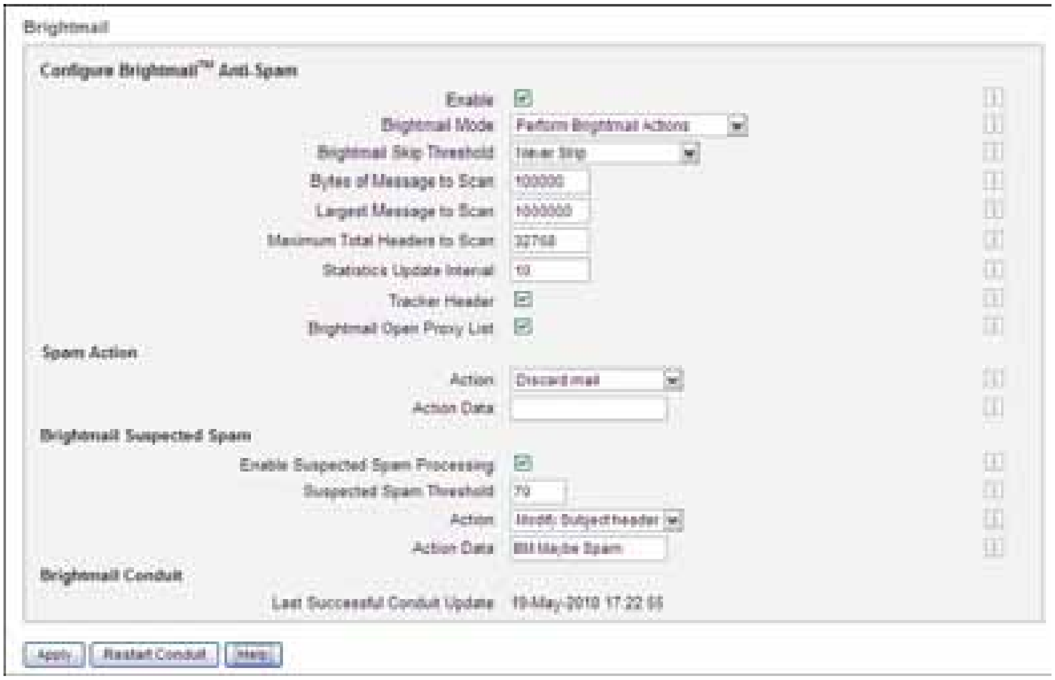
Symantec Brightmail Anti-Spam™ is an add-on subscription that you can run independently from Intercept, or you can fully integrate Brightmail with the Intercept Anti-Spam engine.

You can enable Brightmail for a 30-day evaluation period to allow you to test multi-layered Anti-Spam engines.

Brightmail generates a classification for a message that is used with the Intercept Anti-Spam engine.
A message classified as spam by Brightmail is considered *Certainly Spam* by Intercept and receives a score equal to the *Certainly Spam* threshold. Messages classified as suspected spam by Brightmail are considered Probably Spam in Intercept and receive a score equal to the *Probably Spam* threshold. If a message passes Brightmail scanning as a clean message, it receives an Intercept score of 0. You can also skip Brightmail scanning if Intercept has already classified a message as spam.

To enable and configure Brightmail:

1. Select **Security > Anti-Spam > Brightmail**.
   The Brightmail page appears.



Brightmail

Configure Brightmail™ Anti-Spam

Enable ☑
Brightmail Mode: Perform Brightmail Actions
Brightmail Skip Threshold: Never Skip
Bytes of Message to Scan: 100000
Largest Message to Scan: 1000000
Maximum Total Headers to Scan: 32768
Statistics Update Interval: 10
Tracker Header ☑
Brightmail Open Proxy List ☑

Spam Action

Action: Discard mail
Action Data:

Brightmail Suspected Spam

Enable Suspected Spam Processing ☑
Suspected Spam Threshold: 70
Action: Modify Subject header
Action Data: BM Maybe Spam

Brightmail Conduit

Last Successful Conduit Update: 19-May-2010 17:22:55

2. To enable Brightmail Anti-Spam scanning, select the **Enable** check box.
3. From the **Brightmail Mode** drop-down list, select which mode to run in:

    - **Perform Brightmail Actions** – Brightmail runs independently of Intercept and perform its own actions.
    - **Use in Intercept Spam Decision** – Enable Brightmail for use with the Intercept Anti-Spam engine. The Brightmail scanning result is used in the Intercept Anti-Spam decision for a message.

3. From the **Brightmail Skip Threshold** drop-down list, select when to skip Brightmail processing depending on how Intercept has classified the message.

    - **Never Skip** – Perform Brightmail scanning regardless of previous Intercept scanning results.
    - **Intercept Maybe Spam** – Skip Brightmail scanning for messages already classified by Intercept as *Maybe Spam* or higher.
    - **Intercept Probably Spam** – Skip Brightmail scanning for messages already classified by Intercept as *Probably Spam* or higher.
    - **Intercept Certainly Spam** – Skip Brightmail scanning for messages already classified by Intercept as *Certainly Spam*.

5. In the **Bytes of Message to Scan** text box, type the number of bytes of a message to scan.
   Use a lower number of bytes to increase the scanning speed of Brightmail.
6. In the **Largest Message To Scan** text box, type the largest size of message to scan with Brightmail.

   Messages larger than this value are ignored because spam mail is typically small in size. Scanning large messages also decreases performance.

> ***Note*** *Brightmail processing is skipped if the message size exceeds the threshold, even if the Brightmail Skip Threshold is set to "Never Skip".*

7. In the **Maximum Total Headers to Scan** text box, type the maximum number of headers to scan to prevent messages with many thousands of headers from causing delays in processing.

   The default maximum total number of message headers to scan is set to 32768 bytes. If the maximum is exceeded, the message is classified as spam.

8. In the **Statistics Update Interval** text box, type the interval (in minutes) to send statistics to Brightmail.
   The default interval is set to ten minutes.
9. To enable a tracker header that contains a description of what Brightmail rules apply for a message, select the **Tracker Header** check box.
10. To enable the Open Proxy List feature, select the **Brightmail Open Proxy List** check box.

    The Open Proxy List contains the IP addresses of proxy servers with open or insecure ports. Brightmail blocks all mail coming from any server on this list.

11. From the **Action** drop-down list, select the action to take when Brightmail classifies a message as spam and the mode is set to **Perform Brightmail Actions**.

    - **Just log** – Log the occurrence and take no other action.
    - **Modify Subject Header** – Insert the specified text in the **Action Data** field into the message subject line.
    - **Add header** – Add an "X-" mail header as specified in the **Action Data** field.
    - **Redirect to** – The message is delivered to the mail address or server specified in the **Action Data** field.
    - **Discard mail** – Reject the message and do not send a notification to the sender.
    - **Reject mail** – Reject the message and send a notification to the sender.
    - **BCC**– Send a blind carbon copy of the message to the mail address specified in the **Action Data** field.
    - **Quarantine Mail** – Place the message in the administrative quarantine area.
    - In the **Action Data** text box, type the additional data for the specified action:
    - **Modify Subject Header** – The specified text is inserted into the subject line.
      For example, [BMSPAM].
    - **Redirect to** – Send the message to a mailbox, for example, spam@example.com. You can also redirect the message to a spam quarantine server, for example, spam.example.com.
    - **Add header** – An "X-" message header is added with the specified text, for example, "X-Reject: bmspam". The header action data must start with "X-" and must contain a colon followed by a space.

13. To enable Brightmail suspected spam processing, select the **Enable Suspected Spam Processing** check box.
    Messages detected by Brightmail as suspected spam are classified by Intercept as Probably Spam.
14. In the **Suspected Spam Threshold** text box, type the threshold level to detect suspected spam.
    You can enter values from 25 to 89. Lower numbers are more aggressive. The default value is 70.
15. Click **Apply**.

Brightmail Conduit

Brightmail uses pattern files to match known spam. The Brightmail Conduit feature automatically updates these pattern files to make sure they are always up-to-date.

If you are using an external proxy server to access the Internet, you must configure it in **Configuration > Network > External Proxy Server**.

Note *The first time Brightmail is enabled, it may take 5-10 minutes for the database to initialize. Brightmail updates the rule list incrementally and in some cases it may take up to 24 hours until the rule list is completely up to date.*

11 Spam Quarantine and Trusted/Blocked Senders List

User Spam Quarantine

The WatchGuard XCS Intercept Anti-Spam feature performs actions on spam messages based on their classification. Messages classified as *Certainly Spam* are usually rejected or discarded, while messages classified as *Probably Spam* and *Maybe Spam* are usually quarantined. The administrative quarantine is an area on the system where all quarantined messages are stored, and is only accessible to the administrator.

When spam is filtered and processed, occasionally, a false positive (a legitimate email classified as spam) result can occur. It would be an impossible task for the administrator to examine every message in the quarantine area for messages that are false positives.

The User Spam Quarantine feature redirects spam mail into a local quarantine area for each individual user. With this feature, users can log in to the WatchGuard XCS to see and manage their own quarantined spam. Users can then identify and release any false positives from the quarantine, and delete messages that are actually spam.

Note *The User Spam Quarantine cannot be used in a cluster. We recommend that customers utilize the Quarantine Management Server for large, clustered environments and to support multiple domains.*

Spam Quarantine summary notifications are sent to users to notify them of existing mail in their quarantine. The email notification itself can contain links to take action on messages without the need for the user to log in to the quarantine.

WatchGuard Quarantine Management Server (QMS)

In addition to the local User Spam Quarantine feature of the WatchGuard XCS, organizations can also purchase the WatchGuard QMS (Quarantine Management Server), which is a separate device to which you can redirect spam messages from a WatchGuard XCS.

The WatchGuard QMS is intended for large enterprises, and provides performance improvements to the integrated quarantine services on the WatchGuard XCS because quarantined spam is stored on a separate system. This decreases the processing load and amount of disk space used on the WatchGuard XCS.

The WatchGuard QMS also provides the ability to support multiple domains and clustering, while the WatchGuard XCS User Spam Quarantine feature only supports a single domain.

Local Spam Quarantine Account

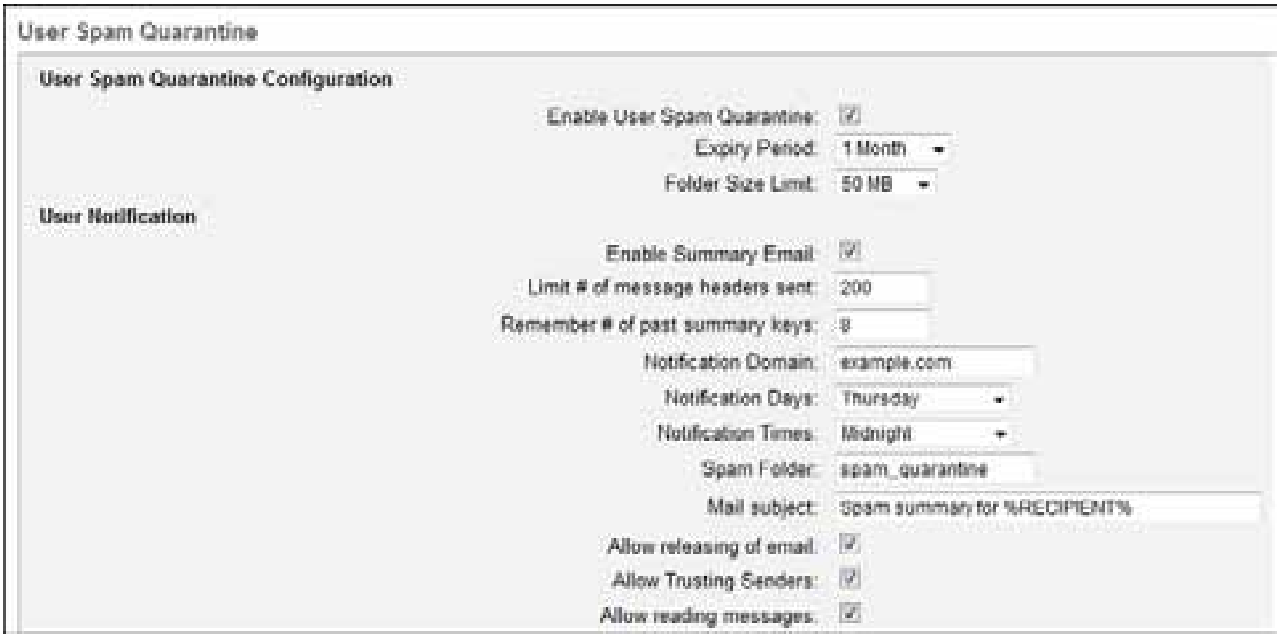
To access quarantined mail, a local account must exist for each user. You can create a local account, or you can use the LDAP Mirrored Users feature to import user accounts from an LDAP compatible directory, for example, Active Directory, and mirror them locally.

See *Directory Users* for more information on importing and mirroring LDAP user accounts.

Configure the Spam Quarantine

To configure the Spam Quarantine:

1. Select **Configuration > WebMail > User Spam Quarantine**.
   The User Spam Quarantine page appears.



User Spam Quarantine

User Spam Quarantine Configuration

Enable User Spam Quarantine: ☑
Expiry Period: 1 Month
Folder Size Limit: 50 MB

User Notification

Enable Summary Email: ☑
Limit # of message headers sent: 200
Remember # of past summary keys: 8
Notification Domain: example.com
Notification Days: Thursday
Notification Times: Midnight
Spam Folder: spam_quarantine
Mail subject: Spam summary for %RECIPIENT%
Allow releasing of email: ☑
Allow Trusting Senders: ☑
Allow reading messages: ☑

2. Select the **Enable Spam Quarantine** check box.
3. From the **Expiry Period** drop-down list, select an expiration period for mail in each quarantine folder.
   Any mail quarantined for longer than the specified value is deleted.
4. From the **Folder Size Limit** drop-down list, select a size, in megabytes, to limit the amount of stored quarantined mail in each quarantine folder.
5. To enable a summary email notification that alerts users to mail that has been placed in their quarantine folder, select the **Enable Summary Email** check box.

6. In the **Limit # of message headers sent** text box, type the maximum number of headers that are sent in the spam digest message.
   Type 0 to send all message headers.
7. In the **Remember # of past summary keys** text box, type the amount of days that users are allowed to access previously sent spam summaries.
   The default is 8.
8. In the **Notification Domain** text box, type the domain for which notifications are sent.
   This is typically the Fully Qualified Domain Name of the email server. The User Spam Quarantine only supports one domain.
9. From the **Notification Days** drop-down list, select the days to send the summary notification.
10. From the **Notification Times** drop-down list, select the time to send the summary notification.

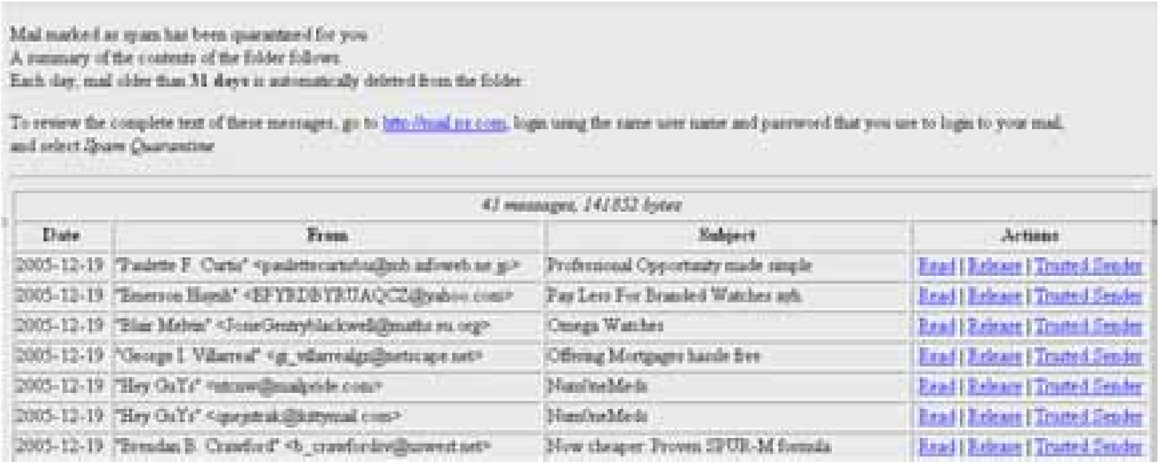
> ***Note*** *The Spam Summary processing begins at this time, but the actual delivery of the summary notifications is not performed until the processing (which may take several minutes) is complete.*

11. In the **Spam Folder** text box, type a folder name for the user’s spam folder.
    This must be an RFC821 compliant mail box name. This folder appears in a user’s mailbox when they receive quarantined spam.
12. In the **Mail Subject** text box, type the subject of the spam summary notification message.
    You can use the WatchGuard XCS system variables in the subject field.
13. To insert a link in the notification summary to allow the user to add the sender to their Trusted Senders List, select the **Allow Trusting Senders** check box.
14. To insert a link in the notification summary to allow the user to read the original message, select the **Allow reading messages** check box.
15. To insert a link in the notification summary to allow the user to release the message to their inbox, select the **Allow releasing of email** check box.
16. In the **Mail Content Preamble** text box, you can edit custom text and HTML versions of the spam summary message that is sent to end users.

    This message contains the links to the user’s quarantined spam. You can use the WatchGuard XCS system variables in the preamble.

Spam Digest Notification

You can send a Spam Digest email notification to alert users to mail that has been placed in their quarantine folder. Additional links in the message allow the end user to read the message, release the message from the quarantine to their inbox, or add the sender to their Trusted Senders list.



Mail marked as spam has been quarantined for you.
A summary of the contents of the folder follows.
Each day, mail older than 31 days is automatically deleted from the folder.

To review the complete text of these messages, go to http://mail.xcs.com, login using the same user name and password that you use to login to your mail, and select *Spam Quarantine*

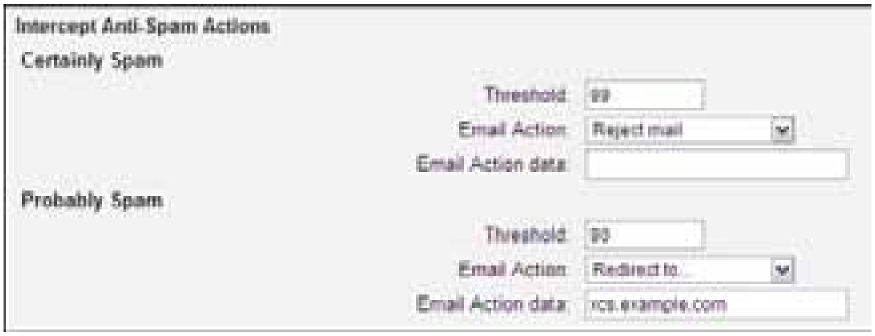
41 messages, 141832 bytes			
Date	**From**	**Subject**	**Actions**
2005-12-19	"Paulette F. Curtis" <paulettecurtisfsa@sch.infoweb.ne.jp>	Professional Opportunity made simple	Read | Release | Trusted Sender
2005-12-19	"Emerson Hanah" <EFYRDBYRUAQCZ@yahoo.com>	Pay Less For Branded Watches aph	Read | Release | Trusted Sender
2005-12-19	"Blair Melvin" <JosieGentryblackwell@maths.ru.org>	Omega Watches	Read | Release | Trusted Sender
2005-12-19	"George I. Villarreal" <gi_villarrealgu@netscape.net>	Offering Mortgages hassle free	Read | Release | Trusted Sender
2005-12-19	"Hey GuYs" <mcow@mailpride.com>	NumOneMeds	Read | Release | Trusted Sender
2005-12-19	"Hey GuYs" <qpeyptrak@kittymail.com>	NumOneMeds	Read | Release | Trusted Sender
2005-12-19	"Brendan B. Crawford" <b_crawfordnv@uswest.net>	Now cheaper: Proven SPUR-M formula	Read | Release | Trusted Sender

Configure Spam Message Redirect Options

To quarantine spam mail to the User Spam Quarantine, you must set the Intercept action to **Redirect to** and set the action data to the address of the spam quarantine server. The **Redirect To** action rewrites the envelope recipient address with the new domain for the quarantine.

To quarantine mail to the spam quarantine:

1. Select **Security > Anti-Spam > Anti-Spam**.



Intercept Anti-Spam Actions

Certainly Spam

Threshold: 99
Email Action: Reject mail
Email Action data:

Probably Spam

Threshold: 80
Email Action: Redirect to...
Email Action data: xcs.example.com

2. Set the **Action** for the spam level that you want to use for the quarantine (for example, *Probably Spam*) to **Redirect to**.
3. Set the **Action data** to the FQDN of the spam quarantine (either this WatchGuard XCS, or another WatchGuard XCS that hosts the User Spam Quarantine.)

   For example, `xcs.example.com`.

4. Click **Apply**.

Access the Spam Quarantine

You can view the quarantine spam folder from the WatchGuard XCS WebMail interface. End users can log in to their local or mirrored account on the WatchGuard XCS and view their own quarantine folder.

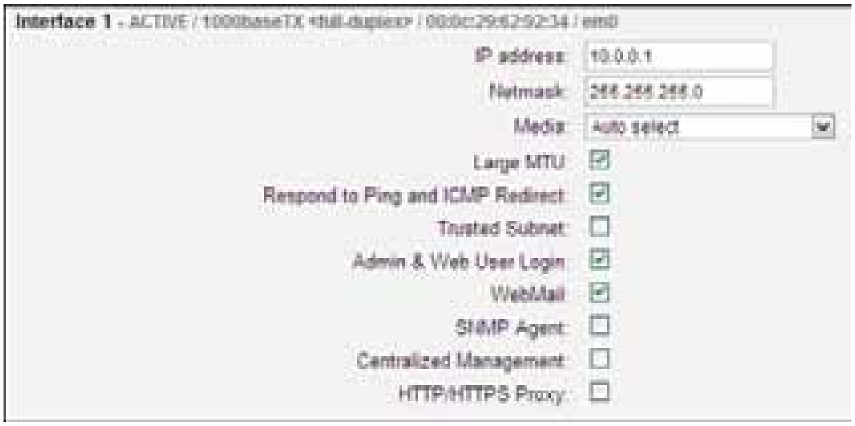
You must enable WebMail access on a network interface in **Configuration > Network > Interfaces** to allow users to log in to the WatchGuard XCS locally or use the linked actions in the spam quarantine digest notification.

If you do not want end users to log in locally to the WatchGuard XCS to retrieve these messages, users can use the linked actions contained in the spam digest notification to manage their quarantined messages.

Enable WebMail and Spam Quarantine Access

To enable WebMail and Quarantine access:

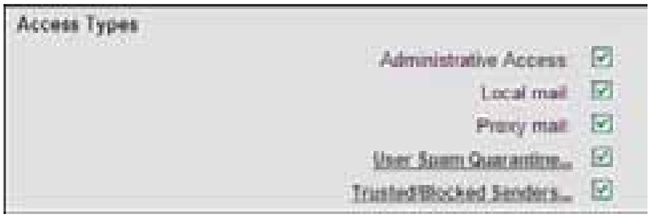
1. Select **Configuration > Network > Interfaces**.
2. Select the **WebMail** check box for the specific network interface that you want to allow users to log in.



Interface 1 - ACTIVE / 1000baseTX <full-duplex> / 00:0c:29:62:92:34 / em0

IP address: 10.0.0.1
Netmask: 255.255.255.0
Media: Auto select
Large MTU: ☑
Respond to Ping and ICMP Redirect: ☑
Trusted Subnet: □
Admin & Web User Login: ☑
WebMail: ☑
SNMP Agent: □
Centralized Management: □
HTTP/HTTPS Proxy: □

3. Click **Apply**.
   You must restart the system.
4. Select **Configuration > WebMail > WebMail**.
5. To provide users with the spam quarantine controls in the WebMail interface, select the **User Spam Quarantine** check box.



Access Types

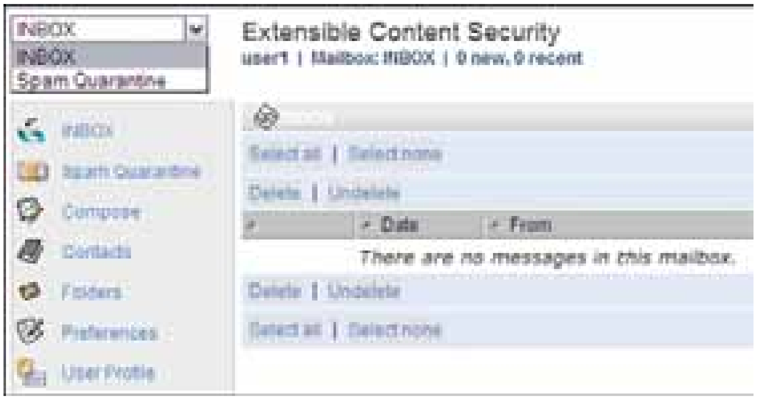
Administrative Access: ☑
Local mail: ☑
Proxy mail: ☑
User Spam Quarantine...: ☑
Trusted/Blocked Senders...: ☑

6. Click **Apply**.

Access the Spam Quarantine with WebMail

To access the quarantine folder with WebMail:

1. Log in to your WatchGuard XCS WebMail account.
2. Select **Spam Quarantine** on the left menu.
   Your user spam quarantine page appears.



Extensible Content Security
user1 | Mailbox: INBOX | 0 new, 0 recent

There are no messages in this mailbox.

When you are in the Spam Quarantine page, you can perform these actions:

- To release the message back into your inbox, click the **Release** link.
- To automatically add the sender to your Trusted Senders List, click the **Trusted Sender** link.
- To automatically add the sender to your Blocked Senders List, click the **Blocked Sender** link.

About Trusted and Blocked Senders Lists

The WatchGuard XCS allows end users to configure their own Trusted and Blocked Senders Lists to control how mail is processed depending on the sender of a message.

Trusted Senders List

The Trusted Senders List allows users to create their own lists of senders that are not blocked by the WatchGuard XCS spam filters. Users can utilize the WebMail interface to create their own Trusted Senders List based on the sender's email address. You can also add Trusted Senders directly from the Spam Quarantine notification message.

The Trusted Senders List overrides these Anti-Spam actions:

- Modify Subject Header
- Add Header
- Redirect

These rules also apply for the Trusted Senders List:

- If the message is rejected for reasons other than spam, for example, viruses or attachment controls, the Trusted Senders List has no effect.
- A **Reject** or **Discard** action rejects or drops the message regardless of the settings in the Trusted Senders List.
- If the action is set to **Just Log** or **BCC**, the trusted message passes through, but is still logged or BCC'd.
- Pattern Filter spam actions set to **Medium** or **High** priority cannot be trusted. This allows you to enforce a strong security policy through higher level priorities.
- The Trusted Senders List cannot trust items rejected during the SMTP connection, for example, rejections because of Reputation Enabled Defense and DNSBL checks.

Blocked Senders List

The Blocked Senders List allows end users to specify a list of addresses from which they do not want to receive mail. These senders are blocked from sending mail to that specific user through the WatchGuard XCS. If a sender is on the Blocked Senders List, the WatchGuard XCS rejects or discards the message.

> ***Note*** *The Trusted Senders List is processed before the Blocked Senders List. If a Blocked Sender also appears in the Trusted Senders List, the email is delivered.*

If there are multiple recipients for a message, and only specific recipients have blocked the sender:

- The message is delivered for those recipients that did not block the sender
- The message is rejected for those who have blocked the sender.

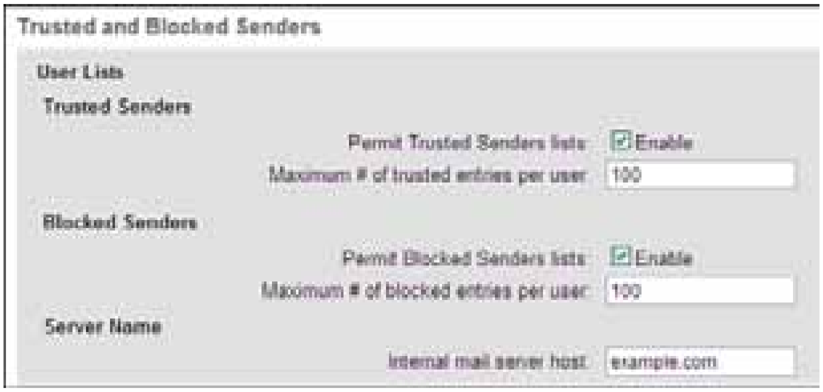
Local users can log in and create their own list of Blocked Senders. Users do not need a local account on the system, as they can be authenticated with LDAP to an authentication server and the user's Trusted/Blocked Senders List is saved locally on the WatchGuard XCS.

Configure the Trusted and Blocked Senders List

You must enable the Trusted and Blocked Senders List feature globally to allow end users to configure their own lists.

To enable the Trusted and Blocked Senders List:

1. Select **Configuration > WebMail > Trusted/Blocked Senders**.
   The Trusted and Blocked Senders List page appears.



Trusted and Blocked Senders

User Lists

Trusted Senders

Permit Trusted Senders lists: ☑ Enable

Maximum # of trusted entries per user: 100

Blocked Senders

Permit Blocked Senders lists: ☑ Enable

Maximum # of blocked entries per user: 100

Server Name

Internal mail server host: example.com

2. Select the **Permit Trusted Senders lists** check box.
3. In the **Maximum # of list trusted entries per user** text box, type the maximum number of users that can be entered on the list.

   The default is 100. Valid values are from 1 to 1000000.

4. Select the **Permit Blocked Senders lists** check box.
5. In the **Maximum # of list blocked entries per user** text box, type the maximum number of users that can be entered on the list.

   The default is 100. Valid values are from 1 to 1000000.

6. In the **Internal mail server host** check box, type the complete host name of the internal mail server or the specified default host name if mail is hosted on this system.

   For example, if you deliver mail to your internal mail server with the address user@example.com, type `example.com`. If your internal mail server uses user@mail.example.com, type `mail.example.com`.

7. From the **Blocked Senders Action** drop-down list, select the action to perform when a user on the Blocked Senders List attempts to send mail through the WatchGuard XCS.

   - **Reject** – Rejects the message and sends a notification to the sender.
   - **Discard** – Discards the message and does not send a notification to the sender.

8. Click **Apply**.

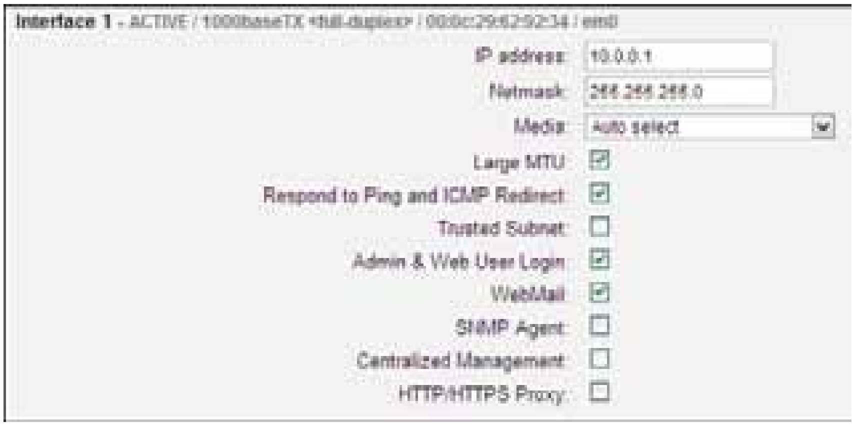
Configure WebMail Access for Trusted/Blocked Senders

You must enable WebMail to allow users to view and edit their Trusted/Blocked Senders List.

Users do not need a local account on the WatchGuard XCS. Users can authenticate with a RADIUS or LDAP authentication server, for example, Active Directory. The user's Trusted/Blocked Senders List is saved locally on the WatchGuard XCS.

To enable WebMail access:

1. Select **Configuration > Network > Interfaces**.
2. Select the **WebMail** check box.

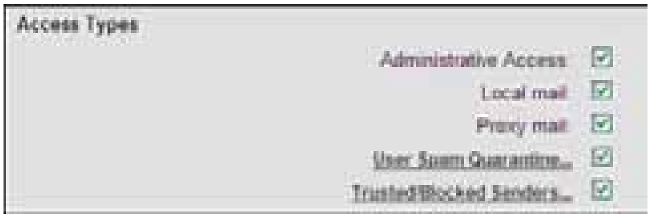


Interface 1 - ACTIVE / 1000baseTX <full-duplex> / 00:0c:29:62:92:34 / em0

IP address: 10.0.0.1
Netmask: 255.255.255.0
Media: Auto select
Large MTU: ☑
Respond to Ping and ICMP Redirect: ☑
Trusted Subnet: □
Admin & Web User Login: ☑
WebMail: ☑
SNMP Agent: □
Centralized Management: □
HTTP/HTTPS Proxy: □

3. Click **Apply**.

   You must restart the system.
4. Select **Configuration > WebMail > WebMail**.
5. Select the **Trusted/Blocked Senders** check box.



Access Types

Administrative Access: ☑
Local mail: ☑
Proxy mail: ☑
User Spam Quarantine...: ☑
Trusted/Blocked Senders...: ☑

6. Click **Apply**.

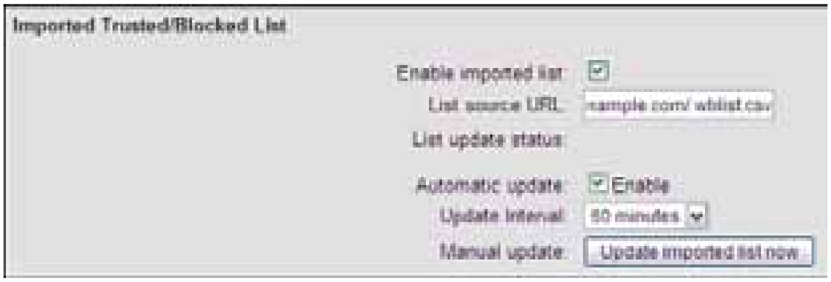
Import Trusted/Blocked Senders List

You can update the Trusted and Blocked Senders Lists manually or automatically from a global list located on an external web server or a Quarantine Management Server (QMS). You can schedule the list update to occur at regular intervals or you can update the list immediately.

We recommend that organizations use either the personal Trusted/Blocked Senders List or the imported list, and not both at the same time.

To import a Trusted/Blocked Senders List:

1. Select **Configuration > WebMail > Trusted/Blocked Senders**.
   The Trusted/Blocked Senders List page appears.



Imported Trusted/Blocked List

Enable imported list: ☑
List source URL: xample.com/ wblist.csv
List update status:
Automatic update: ☑ Enable
Update Interval: 60 minutes
Manual update: Update imported list now

2. In the **Imported Trusted/Blocked List** section, select the **Enable imported list** check box.
3. In the **List source URL** text box, type the URL from which to retrieve the Trusted or Blocked Senders List.

   For example,

   `http://listserver.example.com/wblist.csv`

   For the WatchGuard Quarantine Management Server (QMS), type:

   `http://wqs.example.com/getwblist.spl`

4. To enable scheduled updates, select the **Automatic update** check box.
5. From the **Update Interval** drop-down list, select the time interval for how often to retrieve the list.
6. To immediately perform a manual update, click **Update imported list now**.

Import List File

You can upload a list of Trusted or Blocked Senders in a text file. The file must be in CSV format and contain comma or tab separated entries.

Use this format:

```
[recipient],[sender],[block or trust]
```

For example:

```
user@example.com,spam@example1.com,blockuser@example.com,hacker@example1.com,blockuser@example.com,friend@exa
```

You must use a text editor to create the file bwlist.csv.

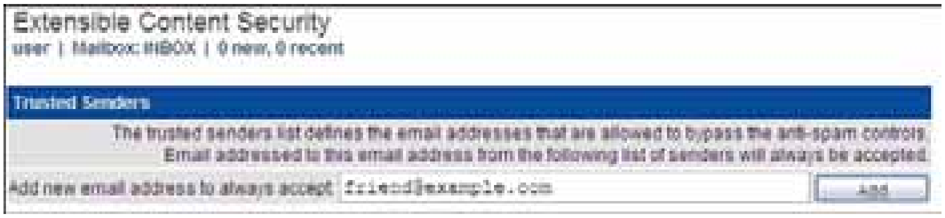
To update a list file:

1. To download the list from the WatchGuard XCS, click **Download File**.
2. Open the file and update the list.
3. Click **Upload File** and upload the edited file to the WatchGuard XCS.

Add Trusted and Blocked Senders

To create a Trusted Senders List:

1. Log in to your WebMail account.
2. Select **Trusted Senders** from the left menu.



Extensible Content Security

user | Mailbox: INBOX | 0 new, 0 recent

Trusted Senders

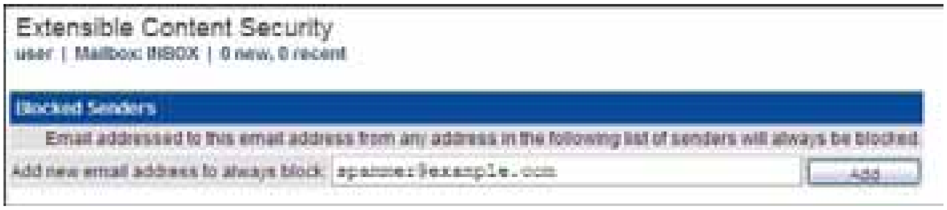
The trusted senders list defines the email addresses that are allowed to bypass the anti-spam controls. Email addressed to this email address from the following list of senders will always be accepted.

Add new email address to always accept: friend@example.com

3. In the **Add new email address to always accept** text box, type an email address.
4. Click **Add**.

To create a Blocked Senders List:

1. Log in to your WebMail account.
2. Select **Blocked Senders** from the left menu.



Extensible Content Security

user | Mailbox: INBOX | 0 new, 0 recent

Blocked Senders

Email addressed to this email address from any address in the following list of senders will always be blocked.

Add new email address to always block: spammer@example.com

3. In the **Add new email address to always block** text box, type an email address.
4. Click **Add**.

12 Policies

About Policies

With policies, specific messaging security features can be customized and applied to different email domains, user groups, IP addresses (Web traffic only), and specific users.

You can use these WatchGuard XCS features with policies:

- Intercept features (Anti-Virus, Spyware, Outbreak Control, Anti-Spam actions and thresholds)
- Content Controls (OCF, Attachment Scanning, Content Scanning, Document Fingerprinting, Content Rules, Pattern Filters)
- Anti-Spam options (Intercept scanners, Component weights)
- Email features (Annotations, Encryption, Archiving, DomainKeys signing)
- Web Proxy features (HTTP/S access, Trusted/Blocked sites, Download/Upload limits, URL Blocking, URL Categorization, Web Reputation)

For example, you can enable Intercept Anti-Spam settings for specific domains, but disable scanning for other domains. Each Anti-Spam action can be customized so that one domain rejects spam messages, while another domain modifies the subject header of a spam message.

Content control actions for inbound and outbound messages can also be specifically defined for the requirements of each domain, group, IP address, or user. For example, you can enable inbound and outbound Content Scanning and Attachment Control checks for some domains, and disable outbound message scanning for other domains.

Specific features can be enabled or disabled independently for email messages and web requests, and separate actions can be applied for inbound and outbound traffic.

In addition, you can add an effective time period to apply to any policy, based on the current time and day of the week.

Sender and Recipient Policy Determination

When a message arrives, the XCS system determines the policy settings for each message recipient with these rules:

- If the message is outbound (trusted), and is addressed to a non-local recipient, then the *sender's* policy settings is used for the recipient.
- If the message is inbound (untrusted), or is trusted but addressed to a local recipient, then the *recipient's* policy settings is used for the recipient.

The *recipient's* policy takes precedence if both the sender and recipient addresses match a policy.

> **Note** *Policy settings are processed after any mail mappings. If the final recipient is a local user, or a user in a domain that the WatchGuard XCS routes mail for, then it is considered a local recipient.*

Policy Hierarchy

There are several types of policies that can apply to a user: User Policy, IP Address Policy, Group Policy, Domain Policy, and Default Policy. Recipients can belong to multiple policies. For example, the recipient user@example.com could have a user-based policy for user@example.com and a policy based on the domain example.com.

The final policy for the recipient is the merged result of any existing policies for that user. Any settings conflicts are resolved in this order:

- User policy (user@example.com)
- IP address policy (10.0.1.100)
- Group policy (Sales)
- Domain policy (example.com)
- Default policy
- Global settings

For example,

If both a user and domain policy apply to a user

- The Anti-Virus feature is enabled in the domain policy
- Anti-Virus is disabled in the user policy

The final result is that Anti-Virus is disabled for the user based on the user policy.

Time Policy

If time policies are configured, a policy with a specific effective time frame takes precedence over a policy with an effective time period of “Always”.

For example,

If a domain has these two domain policies applied to it:

- Policy 1 has an effective time frame of Always
- Policy 2 has an effective time frame of Monday to Friday 9am to 5pm

The final result is that Policy 2 takes effect if the current time is within the effective time period.

Multiple Group Policies

If a user belongs to multiple groups, the imported group order determines the precedence. In the Group Policy configuration page, you can arrange the list of groups into priority order.

For example:

- A user belongs to Group1 and Group2
- Group 1 Policy is set to a higher priority then Group 2 Policy
- Group 1 Policy has Token Analysis enabled
- Group 2 Policy has Token Analysis disabled

The final result is that the user’s email is scanned by Token Analysis.

> ***Note*** *Group policies are not merged as they are with User and Domain policies. If a user belongs to more than one group, only the first group policy in the specified group ordering is applied.*

Pattern Filter Priority

if you use pattern filters with policies, there can sometimes be conflicting priorities for global pattern filters and policy pattern filters. When it processes pattern filter rules, the XCS system makes these decisions:

1. The priorities of all actions are considered. If there is only one High priority action, that filter is used.
2. For pattern filters that have the same priority, policies are resolved in this order:
    - User Policy
    - IP address policy
    - Group policy
    - Domain policy
    - Default policy/Global settings
3. For the same priority and same policy level, actions are resolved in this order:
    - Bypass
    - Reject
    - Discard
    - Quarantine
    - Certainly Spam
    - Redirect
    - Trust
    - Relay
    - Accept
    - Just Log

When you create pattern filters in policies, specific message parts, for example, *Envelope-to* and *Envelope-from*, *Client IP*, and *Host*, are not available. Pattern filters on these message parts cause actions to trigger before the recipients are known, and they are not available for use in policies.

> ***Note*** *BCC and Do Not Train actions do not prevent lower priority actions. For example, a BCC action at “High” priority in the global pattern filter list and an Accept action at “Medium” priority in a policy results in an Accept action and a BCC action.*

Create Policies

These sections describe how to enable and define policies. These are the general steps to create policies:

1. Define global settings
2. Configure the Default policy
3. Add and define new domain, group, IP address, and user policies

Define Global Settings

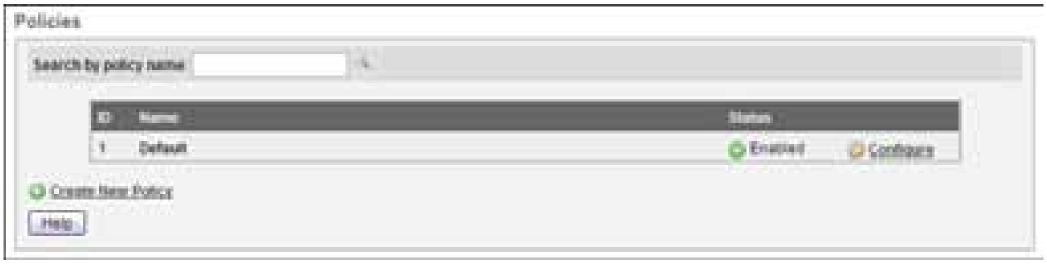
Before you create specific domain, group, IP address, and user policies, we recommend that you define default global settings for Intercept, Anti-Spam, Content Controls, and other features before you define more granular policies based on these global settings.

These settings are inherited by the Default policy. The Default policy is the policy used by all users that do not belong to any other specific policy.

> ***Note*** *If you disable a feature globally, it cannot be enabled by a policy. The feature is completely disabled, regardless of how a policy is configured.*

Configure the Default Policy

1. Select **Security > Policies > Policies**.
   The Policies page appears.

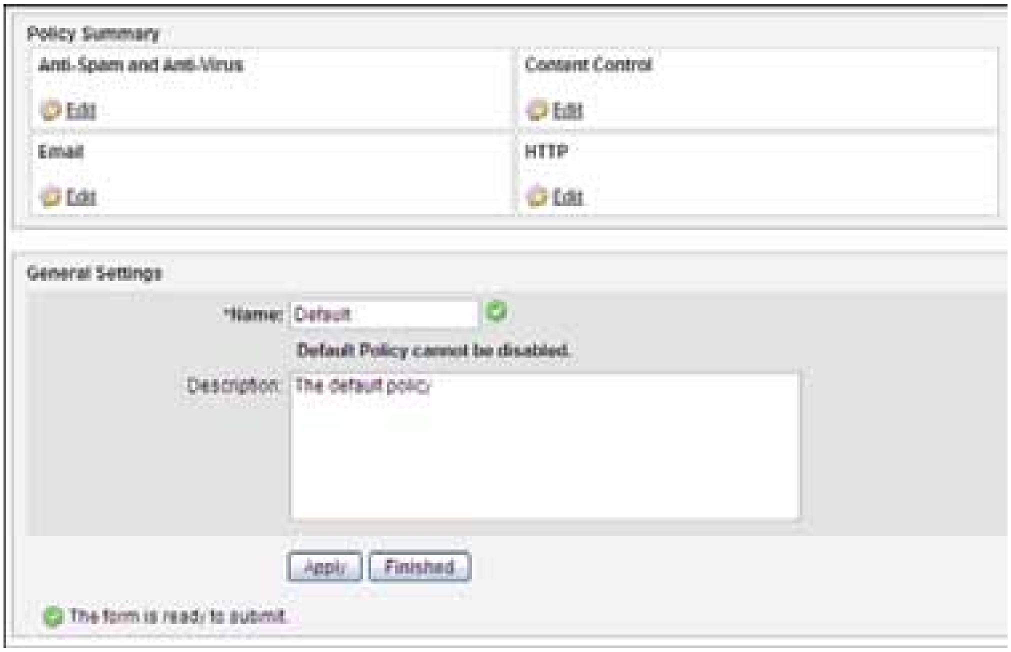


ID	Name	Status	
1	Default	Enabled	Configure

2. Click **Configure** to configure the Default policy.
   The Default Policy summary page appears.

   The features for each policy are displayed in the **Policy Summary** section.

   The display indicates the enabled/disabled status and configured actions for each policy feature.



*Name: Default

Default Policy cannot be disabled.

Description: The default policy

The form is ready to submit.

3. In the **Name** text box, type a descriptive name for this policy.
   For the Default policy, the name can be changed, but the policy cannot be disabled.
4. In the **Description** text box, type a description for the policy.
5. To edit the settings for a feature for this policy, click the **Edit** link for the appropriate category.

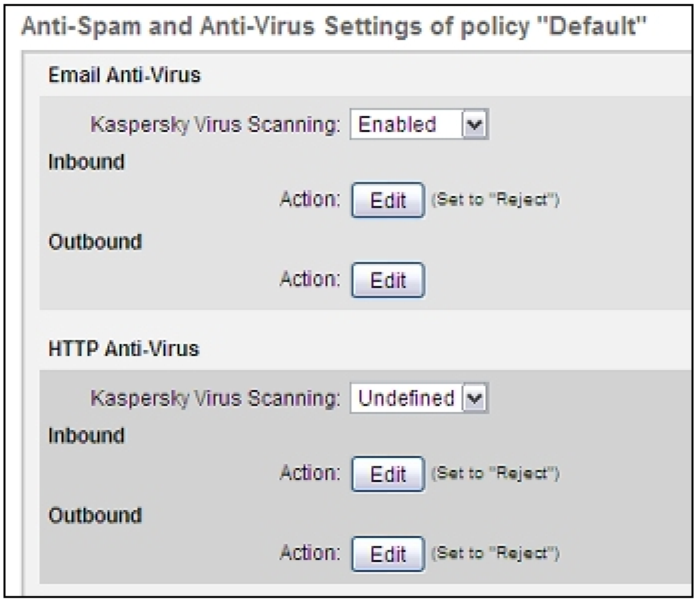
   You can select **Anti-Spam and Anti-Virus**, **Content Control**, **Email**, or **HTTP**.

6. Click **Apply**.

Anti-Spam and Anti-Virus

Configure your settings for this policy for inbound and outbound Anti-Virus, Spyware, Outbreak Control, Malformed Mail, and Anti-Spam.

Select **Enabled** or **Disabled** for each option as required for this policy, or select **Undefined** to use the inherited settings from another policy, the Default policy, or the global settings.



Anti-Spam and Anti-Virus Settings of policy "Default"

Email Anti-Virus

Kaspersky Virus Scanning: Enabled

Inbound

Action: Edit (Set to "Reject")

Outbound

Action: Edit

HTTP Anti-Virus

Kaspersky Virus Scanning: Undefined

Inbound

Action: Edit (Set to "Reject")

Outbound

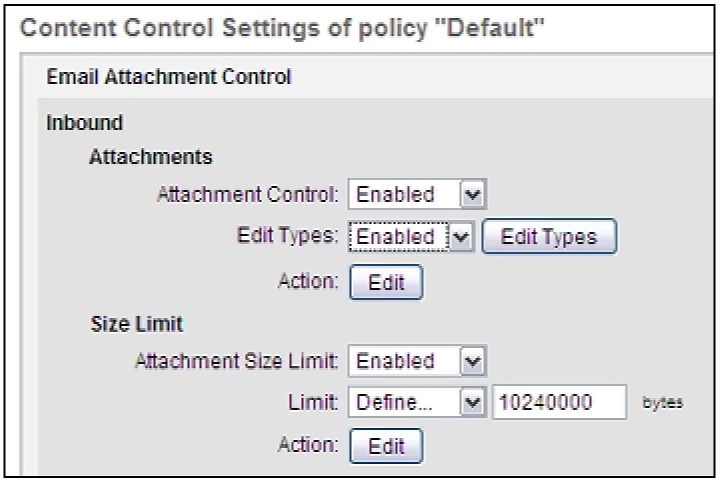
Action: Edit (Set to "Reject")

- **Anti-Virus** – Enable or disable inbound and outbound Anti-Virus for this policy for email and HTTP. You must enable Anti-Virus scanning globally to be used in policies. Independent inbound and outbound actions and notifications can be set for the email and HTTP scanners for this policy.
- **Spyware** – Enable or disable inbound and outbound Spyware detection for this policy for email and HTTP. You must enable Spyware scanning globally to be used in policies. Independent inbound and outbound actions and notifications can be set for the email and HTTP scanners for this policy.
- **Outbreak Control**– Set the inbound and outbound Outbreak Control settings for this policy. You must enable Outbreak Control globally to use this feature in policies. The **Detection Hold Period** is set in hours. The default hold period is 8 hours. In most cases, the Anti-Virus pattern files are updated within 2 to 4 hours of a new virus being discovered. We recommend that you set the hold period for a long enough time to enable the files to be rescanned with updated Anti-Virus pattern files as they become available.
- **Malformed Mail**– Set the Malformed Mail settings for this policy. You must enable Malformed Mail scanning globally to use this feature in policies.
- **Anti-Spam** – Set the Anti-Spam settings for each spam category (**Certainly**, **Probably**, and **Maybe Spam**) for this policy. The **Threshold** spam score for each category can be set between 1-100. (The default global values are: Certainly Spam: 99, Probably Spam: 90, and Maybe Spam: 60). Independent notification actions can be set for the email and HTTP scanners for this policy. You can also configure scanner settings and component weights for each Intercept feature.
- **Scanners** – Enable or disable each Intercept scanner for this policy. You must enable the Intercept scanner globally to be used in policies. For Spam Words, select **Define** in the **Spam Words Dictionaries**section to select your dictionaries. For Weighted Dictionaries, you can enter a custom weight for this policy between 1 and 10000.
- **Brightmail** – Configure the Brightmail settings for this policy. You must license and enable Brightmail globally in **Security > Anti-Spam > Brightmail** to use this feature in policies.
- **Intercept Global Decision Strategy** – Set the Intercept Decision Strategy to use for this policy.
- **Intercept Global Component Weights** – Set the component weights for each Intercept component for this policy. Each weight must be a number between 0 and 100.

Content Control Policy Settings

Configure your Content Control settings for this policy for inbound and outbound Attachment Control, Content Scanning, the Objectionable Content Filter (OCF), and Pattern Filters.

Select **Enabled** or **Disabled** for each option as required for this policy, or select **Undefined** to use the inherited settings from another policy, the Default policy, or the global settings.



Content Control Settings of policy "Default"

Email Attachment Control

Inbound

Attachments

Attachment Control: Enabled

Edit Types: Enabled

Size Limit

Attachment Size Limit: Enabled

Limit: Define... 10240000 bytes

For both inbound and outbound Attachment Control, you can configure these settings:

- **Attachment Control** – Enable or disable Attachment Control for this policy. You must enable Attachment Control globally to be used in policies.
- **Edit Email Types**– Enable or disable the editing of the Attachment Control email types list for this policy. For email, click **Edit Types** to edit the list of attachment types for email for this policy. If disabled, the Attachment Control types list of the default policy or other overriding policy is used.

  For HTTP, click **Edit Types** to edit the list of attachment MIME types for HTTP for this policy. The Web Proxy uses the HTTP Content Header to determine the MIME type of the file, and file extensions should not be entered. If disabled, the Attachment Control types of the Default policy or other overriding policy is used.
- **Action** – Click **Edit** to configure the action to take when a blocked attachment is detected in email traffic. You can enable notifications for the administrator and the user, but you can customize the notification only in the Default policy.

  For HTTP, click **Edit** to configure the specific action to take when a blocked attachment is detected in HTTP traffic. Select **Reject** to reject the message, or **Just Log** to accept the message and record the event in the HTTP Proxy log file. You can enable notifications for the administrator and the user, but you can customize the notification only in the Default policy. Notifications are sent only for a **Reject** action, not **Just Log**.
- **Attachment Size Limits** – Enable or disable Attachment Size Limits for inbound and outbound email messages. Enter the attachment size limit (in bytes). Attachments greater than this threshold trigger the defined **Email Action**. The global default is 10240000 bytes. Set to “0” to indicate no limit.

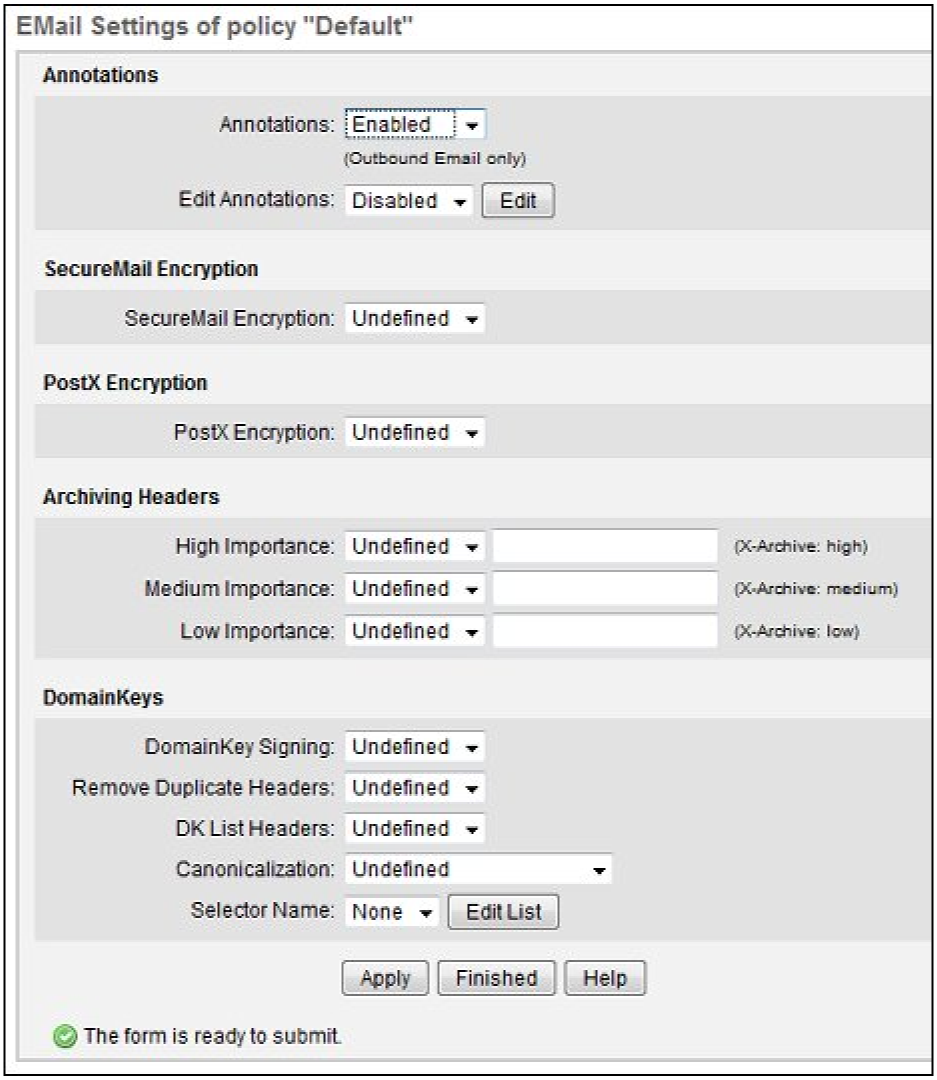
> ***Note*** *The Maximum Message Size configured in* ***Configuration > Mail > Access*** *is also set to 10240000 bytes, and as a result, this threshold is exceeded if the attachment size is close to the attachment size limit. We recommend that the Maximum Message Size value be at least 1.5 times the value of the Attachment Size Limit to make sure that large attachments do not exceed the Maximum Message Size.*

- **Content Scanning** – Set the inbound and outbound Content Scanning settings for email and HTTP for this policy. You must enable Content Scanning globally to use this feature in policies. Select the Compliance dictionaries for use with this policy. For weighted dictionaries, a weighted threshold can be set from 1-10000. You can define independent actions and notifications for the email and HTTP scanners for this policy.
- **Objectionable Content Scanning** – Set the inbound and outbound OCF Scanning settings for email and HTTP for this policy. You must enable OCF globally to use this feature in policies. Select the OCF dictionaries for use with this policy. For weighted dictionaries, a weighted threshold can be set from 1-10000. You can define independent actions and notifications for the email and HTTP scanners for this policy. You can customize notification settings only in the Default policy.
- **Document Fingerprinting** – Enable or disable Document Fingerprinting for this policy. You must enable Document Fingerprinting globally to use this feature in policies. Enter a Document Fingerprinting threshold between 0 and 100. Scores closer to “0” indicate the **Allowed** category. Scores closer to 100 indicate the **Forbidden** category. A score greater than the threshold triggers the specified email action. Document Fingerprinting is applicable only to email messages.
- **Content Rules** – Enable or disable Content Rules for this policy. You must enable Content Rules globally to use this feature in policies. Set the inbound and outbound Content Rules for this policy. You must enable Pattern Filters for Content Rules to work.
- **Pattern Filters** – Click **Pattern Filters** to define email traffic pattern filters for use with this policy. If you disable Pattern Filters in a policy, this action does not disable any globally defined Pattern Filters.

Email Policy Options

Configure your email settings for this policy for the Annotations, PostX Encryption, Archiving, and DomainKeys features.

Select **Enabled** or **Disabled** for each option as required for this policy, or select **Undefined** to use the inherited settings from another policy, the Default policy, or the global settings.



EMail Settings of policy "Default"

Annotations

Annotations: Enabled

(Outbound Email only)

Edit Annotations: Disabled

SecureMail Encryption

SecureMail Encryption: Undefined

PostX Encryption

PostX Encryption: Undefined

Archiving Headers

High Importance: Undefined (X-Archive: high)

Medium Importance: Undefined (X-Archive: medium)

Low Importance: Undefined (X-Archive: low)

DomainKeys

DomainKey Signing: Undefined

Remove Duplicate Headers: Undefined

DK List Headers: Undefined

Canonicalization: Undefined

Selector Name: None

The form is ready to submit.

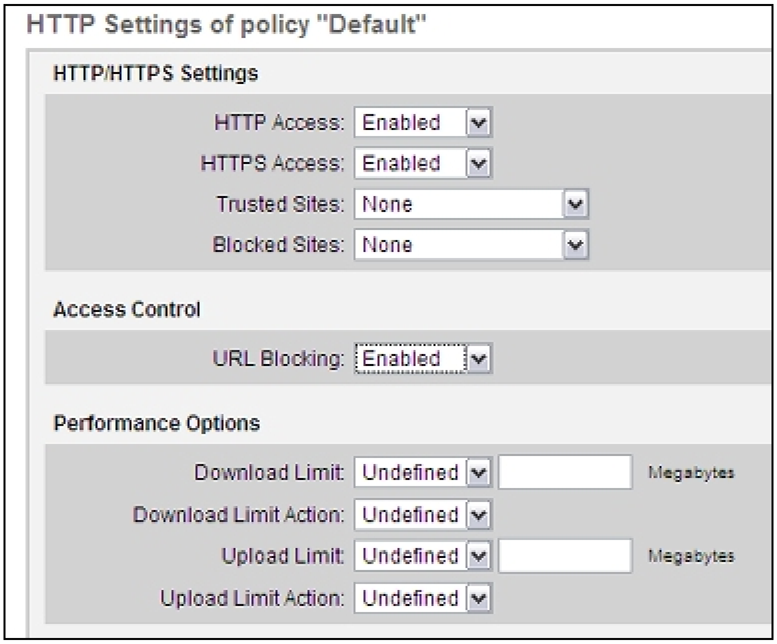
- **Annotations** – Enable or disable annotations for this policy.
- **Edit Annotations** – Enable or disable a customized annotation for this policy. To use a custom annotation with the policy, click **Edit Annotations**. If this option is disabled, the Default policy annotation is used. This annotation is only applied to outgoing mail messages.
- **SecureMail Encryption** – Enable or disable SecureMail encryption for this policy. You must enable SecureMail Encryption globally to use this feature in policies.
- **PostX Encryption** – Enable or disable PostX encryption for this policy. You must enable PostX Encryption globally to use this feature in policies.
- **Archiving Headers** – Set any archive headers (for High, Medium, and Low Priority) for this policy. A correct X header must be used, for example, *X-Archive: high*. You must enable Archiving globally to use this feature with policies.
- **DomainKeys** – Set the DomainKeys configuration for this policy. You must enable DomainKeys globally to use this feature with policies. To edit the list of selector names that are used with the policy, click **Edit List**.

HTTP Policy Options

You must enable the Web Proxy before you can use the feature in policies.

Select **Enabled** or **Disabled** for each option as required for this policy, or select **Undefined** to use the inherited settings from another policy, the Default policy, or the global settings.

> ***Note*** *If the HTTP and HTTPS Access fields are "Undefined", they inherit the state of the global setting for the HTTP Proxy (enabled or disabled).*



HTTP Settings of policy "Default"

HTTP/HTTPS Settings

HTTP Access: Enabled
HTTPS Access: Enabled
Trusted Sites: None
Blocked Sites: None

Access Control

URL Blocking: Enabled

Performance Options

Download Limit: Undefined Megabytes
Download Limit Action: Undefined
Upload Limit: Undefined Megabytes
Upload Limit Action: Undefined

- **HTTP Access** – Enables the Web Proxy to control and manage access to external web sites.
- **HTTPS Access** – Enables the Web Proxy to control and manage access to external web sites with HTTPS. Content inspection cannot be performed on HTTPS traffic.
- **Trusted Sites** – The Trusted Sites list allows the administrator to upload a list of specific web sites that bypass all scan features. These feature include Anti-Virus, HTTP content control features (Attachment Control, Objectionable Content, Content Scanning), and URL filtering features (URL Blocking and URL Categorization). Trusted Sites lists are configured with the Dictionaries & Lists feature. Use a domain type list that contains a list of domains and IP addresses.

  For example,

  `example1.comexample.2com192.168.1.128.`

- **Blocked Sites** – Select a predefined list of Blocked Sites, or set to **None** to allow all sites. The Blocked Site list is configured through the Dictionaries & Lists feature. The Web Proxy blocks these sites for all users.

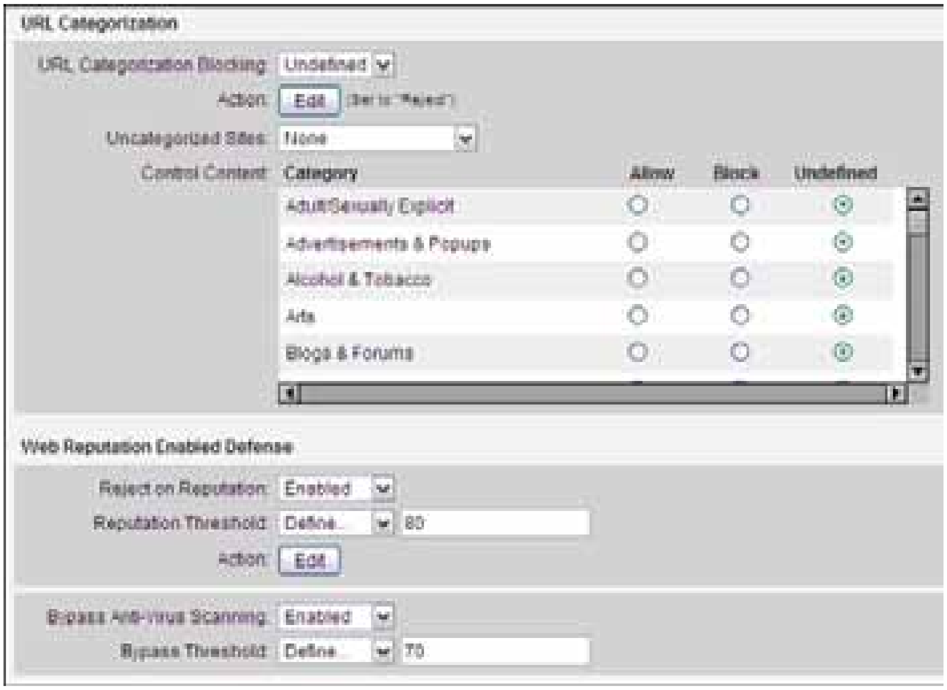
  Use a domain type list that contains a list of domains and IP addresses.

  For example,

  `example1.comexample.2com192.168.1.128`

> **Note** *If a site appears in both the Trusted and Blocked Sites lists, the Trusted Sites list takes precedence.*

- **URL Blocking** – Enables URL blocking to block access to web sites that appear on a URL Block List.
- **Upload and Download Limit** – Enter the size limit (in megabytes) for HTTP downloads and uploads. The default is 7 MB. Keep the field clear or set it to “0” for no limit. Files larger than this size are bypassed or blocked depending on the configured action.
- **Download and Upload Limit Action**– Set the **Download Limit Action** and **Upload Limit Action** to apply when the message exceeds the size threshold:
  - **Undefined** – Any limits and actions on downloads and uploads use the inherited settings from another overriding policy or the default policy.
  - **Block** – The file transfer is blocked and an error message is sent to the web client to indicate the reason the download or upload is blocked.
  - **Bypass** – The file transfer is not blocked and bypasses any HTTP content scans. This allows larger files to be uploaded or downloaded, but prevents the use of too many scanning resources because of their size. This is the default value.
- **URL Categorization** – Enables URL Categorization for use with this HTTP policy. URL Categorization prevents HTTP access to web sites with a predefined list of blocked web sites organized in several topic categories.



URL Categorization

URL Categorization Blocking: Undefined

Action: Edit (Set to "Reject")

Uncategorized Sites: None

Control Content:

Category	Allow	Block	Undefined
Adult/Sexually Explicit	○	○	●
Advertisements & Popups	○	○	●
Alcohol & Tobacco	○	○	●
Arts	○	○	●
Blogs & Forums	○	○	●

Web Reputation Enabled Defense

Reject on Reputation: Enabled

Reputation Threshold: Define... 80

Action: Edit

Bypass Anti-Virus Scanning: Enabled

Bypass Threshold: Define... 70

  - You can enable or disable each web site category in this policy. You can also configure the HTTP action for connections blocked by URL Categorization.
  - From the **Uncategorized Sites** drop-down list, select a list that contains the web site domains that are not categorized by URL Categorization.

> **Note** *Any web sites defined in the Trusted or Blocked Sites list override URL Categorization blocking.*

- **Web Reputation Enabled Defense** – Enable or disable Web Reputation for this policy or select **Undefined** to use the inherited value from another policy, the Default policy, or the global settings.
  - From the **Reputation Threshold** drop-down list, select **Define** to enter a value, or select **Undefined** to use the inherited value from another policy, the Default policy, or the global settings.
  - In the **Action** field, click **Edit** to define an action to perform if a web site reputation score exceeds the configured **Reputation Threshold**.
  - From the **Bypass Anti-Virus Scanning**, drop-down list, enable or disable the option to bypass Anti-Virus scanning for web connections if the reputation of the requested web site is below the specified threshold.
  - From the **Bypass Anti-Virus Threshold** drop-down list, select **Define** and type a threshold below which web sites bypass Anti-Virus scanning, or select **Undefined** to use the inherited value from another policy, the Default policy, or the global settings.

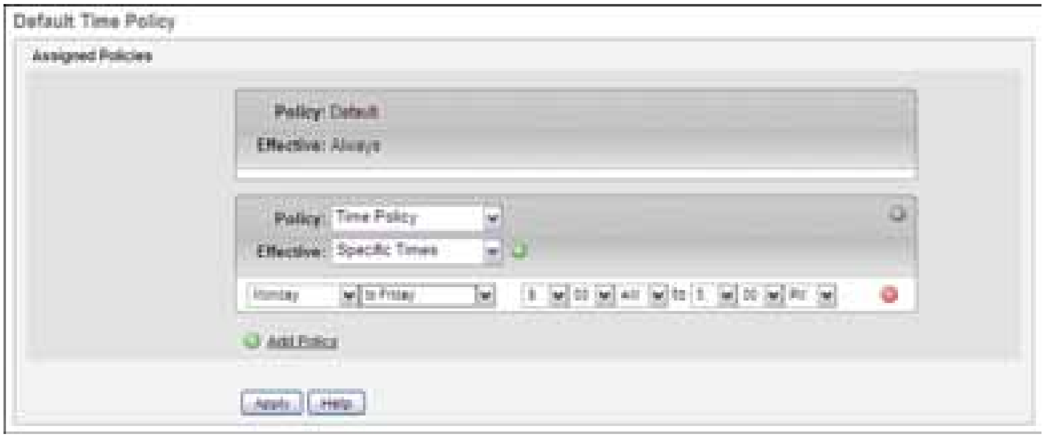
Default Time Policy

Time-based policies enable policies to be applied based on the current time and day of the week. Time-based policies are configurable for user policies, IP address policies, group policies, domain policies, and the Default policy.

The Default Time Policy takes effect for a message if no other policy applies.

The Default Policy is set for an effective time period of **Always** and cannot be changed. Any Default Time Policies you add overrides the Default Policy.

1. Select **Security > Policies > Default Time Policy**.
   The Default Time Policy page appears.



Default Time Policy

Assigned Policies

Policy: Default
Effective: Always

Policy: Time Policy
Effective: Specific Times

Monday to Friday 8 : 00 AM to 5 : 00 PM

2. Click **Add Policy**.
3. From the **Policy** drop-down list, select an existing policy to add.
4. From the **Effective** drop-down list, select **Specific Times** to configure the time periods for which this policy takes effect, or select **Always** for no time restriction.
   Click the "+" symbol to add additional time periods.
5. Click **Add Policy** to add additional default time policies, if required.
6. Click **Apply**.

Define Domain, Group, IP Address, and User policies

When global settings and Default policy settings are defined, administrators can create and define policies for domains, groups, IP addresses, and users.

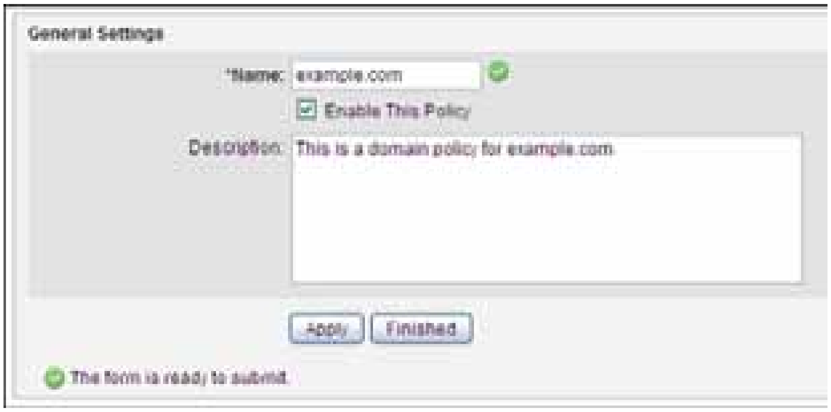
These policies are described in detail in the subsequent sections.

Domain Policies

You can define domain policies to enable different policies for different domains in an organization.
For example, you can create a policy to assign annotations to different email domains that require separate annotations (for example, a legal disclaimer) appended to their messages.

To create a domain policy:

1. Select **Security > Policies > Policies**.
   The Policies page appears.
2. Click **Create New Policy**.



General Settings

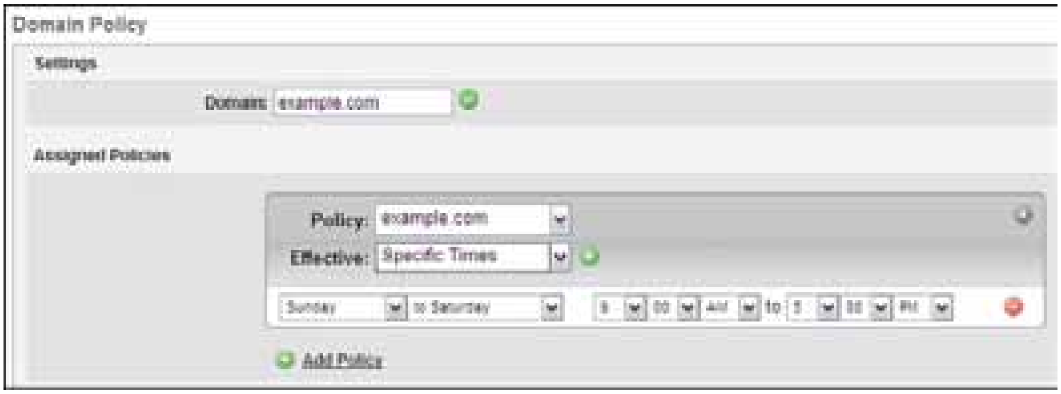
*Name: example.com

☑ Enable This Policy

Description: This is a domain policy for example.com

The form is ready to submit.

3. In the **Name** text box, type a name for this policy, for example, `example.com`.
4. Select the **Enable This Policy** check box.
5. In the **Description** text box, type a detailed description for this policy.
6. Customize the policy as required by selecting the feature tabs, for example, **Anti-Virus and Anti-Spam**, **Content Controls**, **Email**, and **HTTP**.
7. For example, to customize an annotation for this domain policy, select the **Email** section.
8. From the **Annotations** drop-down list, select **Enabled**.
9. Click the **Edit Annotations** button to customize the annotation that is appended to messages for this domain.
10. Click **Apply**.
11. Click **Apply** to save the domain policy.
12. Select **Security > Policies > Domain Policy**.
    The Domain Policy page appears.



Domain Policy

Settings

Domains: example.com

Assigned Policies

Policy: example.com

Effective: Specific Times

Sunday to Saturday 8 00 AM to 5 30 PM

13. In the **Domain** text box, type the domain to which this policy applies.

    For example, `example.com`

    Use a leading "." to indicate subdomains of the specified domain.

    For example, `.example.com`

    matches these domains: `a.example.com, b.example.com, c.d.example.com`, but not `example.com`.
14. From the **Policy** drop-down list, select the policy to apply to the specified domain.
15. From the **Effective** drop-down list, select **Specific Times** to configure the time periods for which this policy takes effect, or select **Always** for no time restriction.
    Click the "+" symbol to add additional time periods.
16. Click **Add Policy** to add additional policies for this domain.
    You can add up to five policies.
17. Click **Apply**.

Upload and Download Domain Policy Lists

You can upload a list of domain policy assignments in a text file. The file must contain comma or tab separated entries with one entry on each line.

Use this format:

```
[Domain],[policy],[startday],[starthr],[startmin],[stopday],[stophr],[stopmin]
```

Days are specified by a number from 0 to 6, starting with Sunday (0). Hours are specified in 24-hour format with a number from 0 to 23. Minutes are specified in these increments: 0,15,30,45.

For example:

```
example.com,-
Example1Policy,1,9,0,5,17,0example2.com,Example2Policyexample3.com,Example3Policy,0,8,0,4,12,0
```

You must use a text editor to create the file domain_policy.csv.

To update a domain policy text file:

1. To download the domain policy list from the WatchGuard XCS, click **Download File**.
2. Open the file and update the domain policy list.

3. Click **Upload File** and upload the edited file to the WatchGuard XCS.

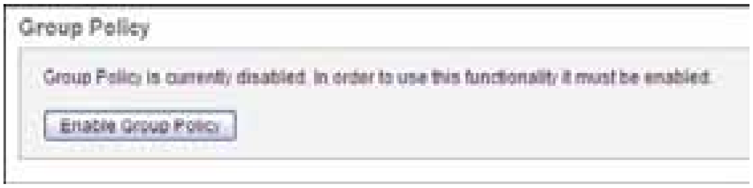
Group Policies

You can customize policies for users who belong to specific groups. For example, a Sales group can have different content scanning policies than users in the Development group. Group policies are also useful for providing different annotations or Anti-Spam scanning features for each user group.

Enable Group Policy

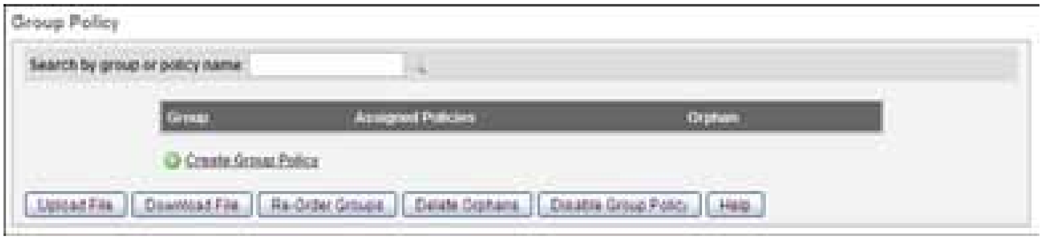
Before you import users and groups, enable Group policy to make sure the imported groups are displayed in the group policy page. If the Group policy option is enabled after you import group membership information, you must wait until the next scheduled import, or perform a manual import, before the list of groups appear on this page.

1. Select **Security > Policies > Group Policy**.
   The Group Policy page appears.



Group Policy is currently disabled. In order to use this functionality it must be enabled.

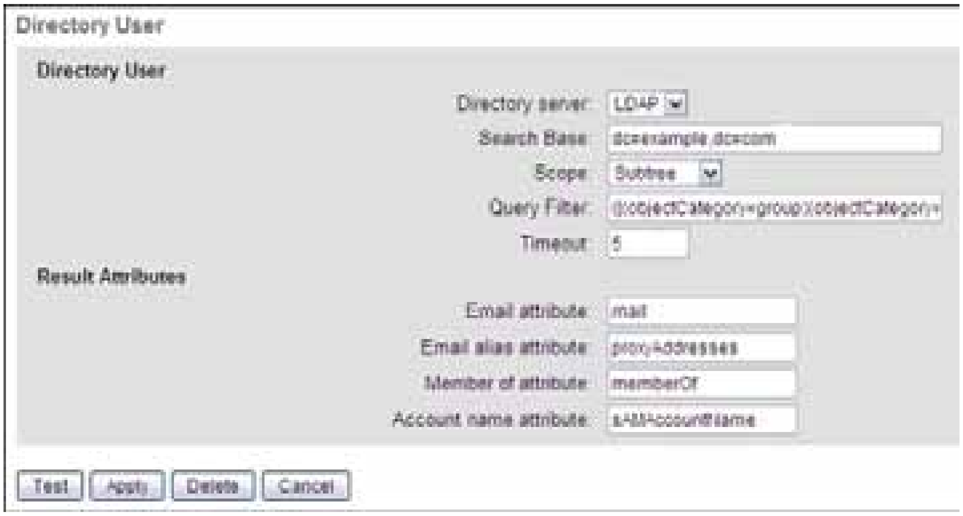
2. Click **Enable Group Policy**.
   The Group Policy configuration page appears.



Import LDAP Group Information

Before you configure Group policy, you must first import group membership information from an LDAP directory server.

1. Select **Configuration** > **LDAP > Directory Users**.
   The Directory Users page appears.



Directory User

Directory User

Directory server: LDAP

Search Base: dc=example,dc=com

Scope: Subtree

Query Filter: (|(objectCategory=group)(objectCategory=

Timeout: 5

Result Attributes

Email attribute: mail

Email alias attribute: proxyAddresses

Member of attribute: memberOf

Account name attribute: sAMAccountName

2. From the **Directory Server** drop-down list, select a configured server.
3. In the **Search Base** text box, type a path to start the search from.

   For example: `dc=example,dc=com`.

4. From the **Scope** drop-down list, select the scope for the search.

   - **Base** – Searches the base object only.
   - **One Level** – Searches objects beneath the base object, but excludes the base object.
   - **Subtree** – Searches the entire subtree, of which the base distinguished name is the topmost object, and includes the base object.

5. In the **Query Filter** text box, type the appropriate filter for your LDAP server.

   For Active Directory use:

   ```
   (|(|(objectCategory=group)(objectCategory=person))(objectCategory=publicFolder))
   ```

   This query filter includes mail-enabled Exchange public folders to prevent them from rejection if *Reject on Unknown Recipient* is enabled.

   For iPlanet and OpenLDAP, use the`(objectClass=person)` query filter.

6. In the **Timeout** text box, enter the maximum interval, in seconds, to wait for the search to complete.
   You can enter values from 1 to 100 seconds.
7. In the **Email attribute** text box, type the attribute that identifies the email address of the user.

   For Active Directory, iPlanet, and OpenLDAP, type `mail`.

8. In the **Email alias attribute** text box, enter the attribute that identifies alternate email addresses for the user.

   For Active Directory, type `proxyAddresses`.

   For iPlanet, type `Email`. For OpenLDAP, leave this field blank.

9. In the **Member Of** text box, type the attribute that identifies the groups to which the user belongs.

   For Active Directory, type `memberOf`.

   For iPlanet, type `Member`. For OpenLDAP, leave this field blank.

10. In the **Account Name Attribute** text box, type the attribute that identifies an account name for the user for login.

    In Active Directory, type *sAMAccountName*.

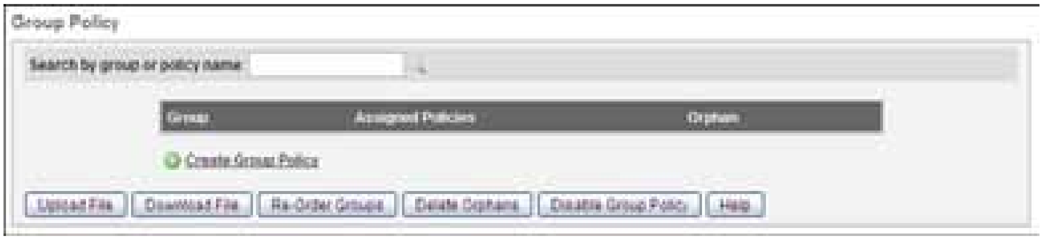
    For iPlanet, use `uid`. For OpenLDAP, use `cn`.
11. Click **Apply**.
12. Click **Import Now** to import users and their corresponding group memberships from an LDAP directory.

    Click **Import Settings** to set up scheduled imports.

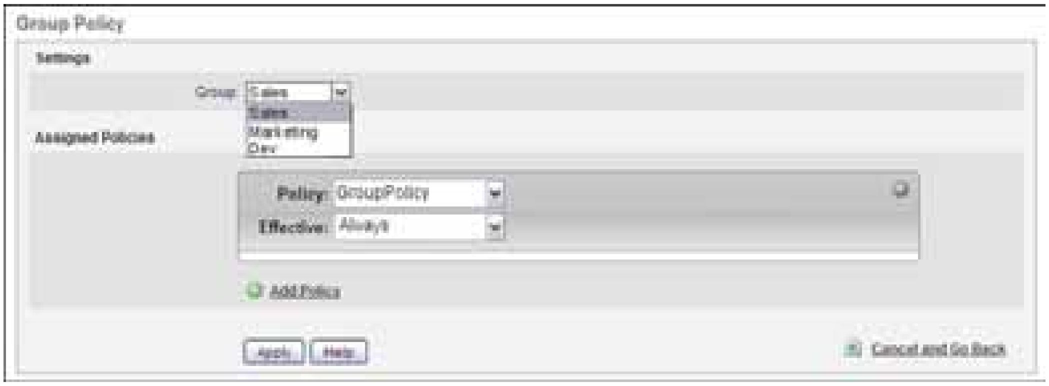
Configure Group Policy

After you import group and user information from an LDAP directory server, you can configure Group policies.

1. Select **Security > Policies > Group Policy**.
   The Group Policy page appears.



2. Select **Create Group Policy**.



Group: Sales

Policy: GroupPolicy

Effective: Always

3. From the **Group** drop-down list, select an existing group.
4. From the **Policy** drop-down list, select the policy to apply to the specified group.
5. From the **Effective** drop-down list, select **Specific Times** to configure the time periods for which this policy takes effect, or select **Always** for no time restriction.
   Click the "+" symbol to add additional time periods.
6. Click **Add Policy** to add additional policies for this group.
   You can add up to five policies.
7. Click **Apply**.

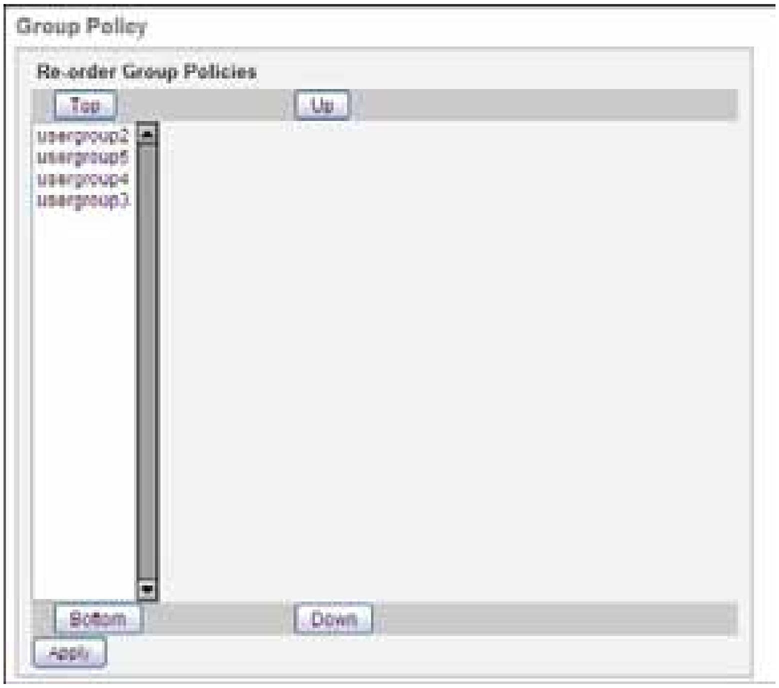
Re-order Groups

If the user belongs to more than one group, group policies are applied in the order the groups are imported.

For example, in the case of annotations, the annotation used for a user who belongs to multiple groups is the annotation for their first group that appears in the group order.

To re-order groups:

1. Click **Re-order Groups**.
   The Re-order Group Policies page appears.



2. Select a group to move.

> ***Note*** *Only groups assigned to a policy are displayed.*

3. Click **Up** or **Down** to move the group up and down the list order.

   Click **Top** and **Bottom** to move the selected group to the top or bottom of the list.
4. When you have finished the re-ordering of groups, click **Apply**.

Orphaned groups

Orphaned LDAP groups are groups that have been deleted from the LDAP directory but still exist in the local group list. Any policies configured for these orphaned groups are not processed.

To remove orphaned groups from the Group policy page, click **Delete Orphans**.

Upload Group Policy Lists

You can upload lists of group policy assignments in a text file. The file must contain comma or tab separated entries with one entry per line.

Use this format:

```
[group],[policy],[startday],[starthr],[startmin],[stopday],[stophr],[stopmin]
```

Days are specified by a number from 0 to 6, starting with Sunday (0). Hours are specified in 24-hour format with a number from 0 to 23. Minutes are specified in these increments: 0,15,30,45.

For example:

```
sales,salespolicy,1,9,0,5,17,0marketing,marketingpolicydev,devpolicy,0,8,0,4,12,0
```

You must use a text editor to create the file group_policy.csv.

To update a group policy text file:

1. To download the group policy list from the WatchGuard XCS, click **Download File**.
2. Open the file and update the group policy list.
3. Click **Upload File** and upload the edited file to the WatchGuard XCS.

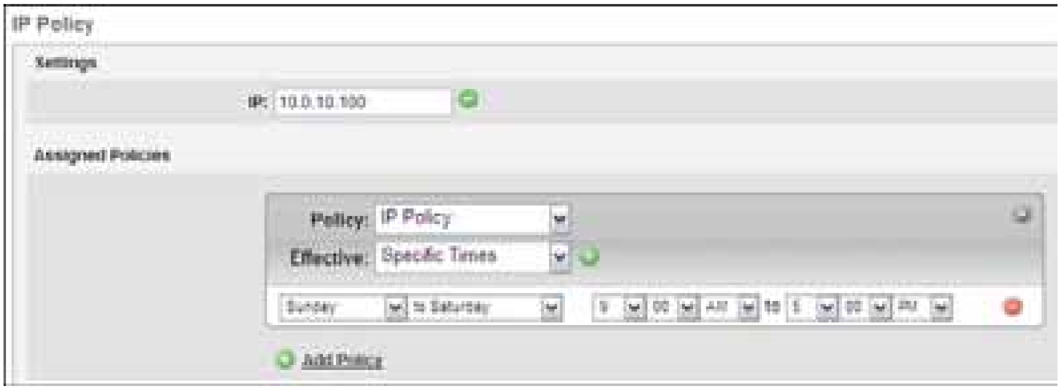
IP Address Policies

You can customize web policies for specific IP addresses or networks. IP address-based policies take precedence over domain and group policies, but can be overridden by a user policy.

IP address policies are specifically for web traffic only, and apply to the IP address of the web browser client, or the IP address of an intermediary HTTP proxy that is positioned between web clients and the WatchGuard XCS.

> ***Note*** *IP address policies are not used for email messages.*

1. Select **Security > Policies > IP Policy**.
   The IP Policy page appears.



IP Policy

Settings

IP: 10.0.10.100

Assigned Policies

Policy: IP Policy

Effective: Specific Times

Sunday to Saturday 9 : 00 AM to 5 : 00 PM

2. In the **IP** text box, enter the IP address or network to which to apply the policy.

You must enter a valid IP address or network using CIDR/slash notation. The WatchGuard XCS automatically adds the network /32 for a single IP address.

For example, to enter an IP address, type `10.0.10.100`

To enter a network, use slash notation. For example, type `10.1.0.0/16`

3. From the **Policy** drop-down list, select the policy to apply to the specified IP address or network.
4. From the **Effective** drop-down list, select **Specific Times** to configure the time periods for which this policy takes effect, or select **Always** for no time restriction.
   Click the "+" symbol to add additional time periods.
5. Click **Add Policy** to add additional policies for this IP address or network.
   You can add up to five policies.
6. Click **Apply**.

Upload and Download IP Address Policy Lists

You can upload a list of IP address policy assignments in a text file. The file must contain comma or tab separated entries with one entry on each line.

Days are specified by a number from 0 to 6, starting with Sunday (0). Hours are specified in 24-hour format with a number from 0 to 23. Minutes are specified in these increments: 0,15,30,45.

Use this format:

```
[IP/Net],[policy],[startday],[starthr],[startmin],[stopday],[stophr],[stopmin]
```

You must enter single IP addresses using CIDR/slash notation with the network /32, for example, 10.1.1.10/32.

For example:

```
10.0.1.10/-
32,IPPolicy1,1,9,0,5,17,010.1.0.0/16,IPNetPolicy10.0.10.100/32,IPPolicy2,0,8,0,4,12,0\
```

You must use a text editor to create the file ip_policy.csv.

To update an IP address policy text file:

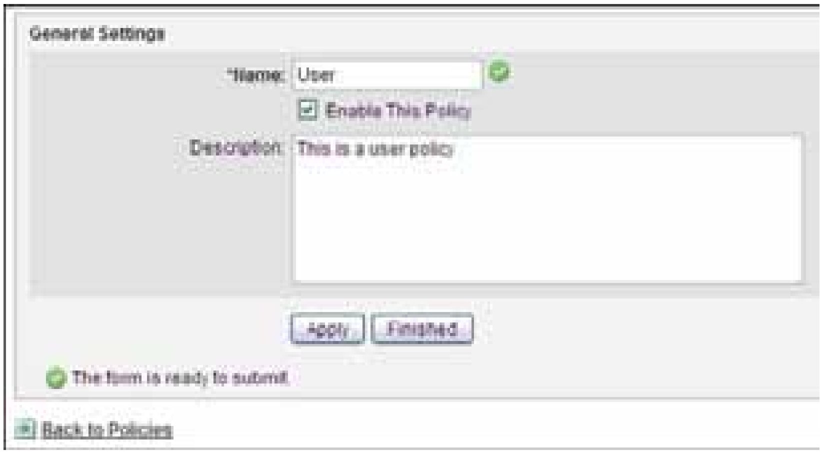
- To download the IP address policy list from the WatchGuard XCS, click **Download File**.
- Open the file and update the IP address policy list.
- Click **Upload File** and upload the edited file to the WatchGuard XCS.

User Policies

You can customize policies for individual user email addresses. User policies take precedence over domain, IP address, and group policies, and are useful for to create individual exceptions to these policies.

In this example, we create a user policy with custom Anti-Virus settings.

1. Select **Security > Policies > Policies**.
   The Policies page appears.
2. Click the **Create New Policy** link.
   The Policy Settings page appears.



General Settings

*Name: User

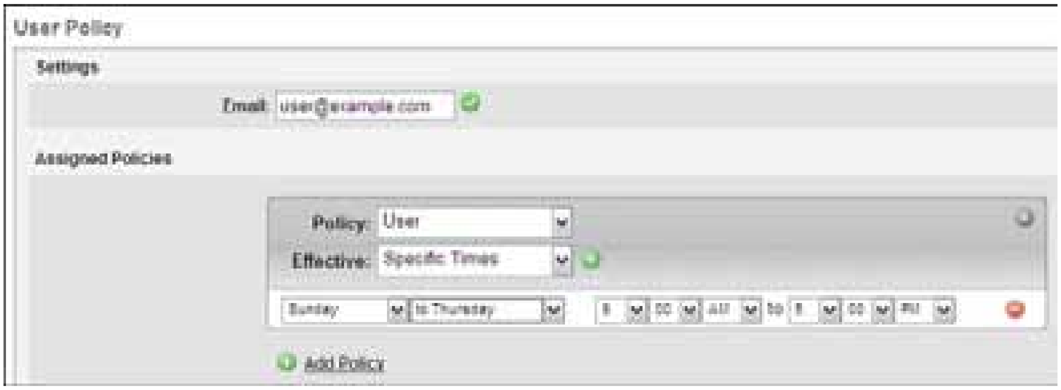
☑ Enable This Policy

Description: This is a user policy

The form is ready to submit.

3. In the **Name** text box, type a name for this policy.
4. Select the **Enable This Policy** check box.
5. In the **Description** text box, type a detailed description for this policy.
6. To customize the Anti-Virus settings for both inbound and outbound directions for this user policy, select **Anti-Spam and Anti-Virus** and make any required changes to the policy.
7. Click **Apply**.
8. Select **Security > Policies > User Policy**.

   The User Policy page appears.



User Policy

Settings

Email: user@example.com

Assigned Policies

Policy: User

Effective: Specific Times

Sunday to Thursday 8 00 AM to 5 00 PM

9. In the **Email** text box, type the email address of the user.
10. From the **Policy** drop-down list, select the policy to apply to the specified user.
11. From the **Effective** drop-down list, select **Specific Times** to configure the time periods for which this policy takes effect, or select **Always** for no time restriction.

    Click the "+" symbol to add additional time periods.
12. Click **Add Policy** to add additional policies for this user.

    You can add up to five policies.
13. Click **Apply**.

Upload and Download User Policy Lists

You can upload a list of user policy assignments in a text file. The file must contain comma or tab separated entries with one entry on each line.

Days are specified by a number from 0 to 6, starting with Sunday (0). Hours are specified in 24-hour format with a number from 0 to 23. Minutes are specified in these increments: 0,15,30,45.

Leave the time fields blank if the effective time is set to **Always**.

Use this format:

```
[email],[policy],[startday],[starthr],[startmin],[stopday],[stophr],[stopmin]
```

For example:

```
user@exam-
ple.com,User1Policy,1,9,0,5,17,0user2@example.com,User2Policyuser3@example.com,User3Policy,0,8,0,4,1
```

You must use a text editor to create the file email_policy.csv.

To update a user policy text file:

1. To download the user policy list from the WatchGuard XCS, click **Download File**.
2. Open the file and update the user policy list.
3. Click **Upload File** and upload the edited file to the WatchGuard XCS.

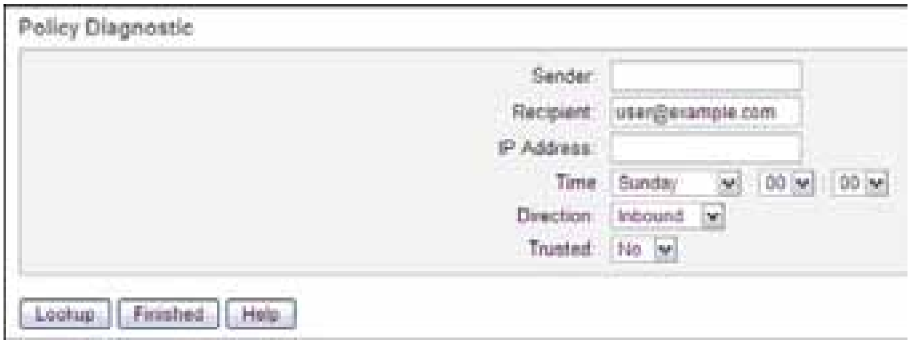
Policy Diagnostics

From the *Policy Diagnostics* page, you can test your policy structure and make sure the final result for a specific user is the desired result. There are several policies that can apply to a single user: domain policies, user policies, IP address policies, group policies, time policies, and the Default policy.

You can enter the sender and recipient's email address, the IP address, the time period, direction and trusted level of the message. The policy diagnostic page displays each policy feature and includes information on which policies were overridden by another policy with higher priority.

To run policy diagnostics:

1. Select **Security > Policies > Diagnostics**.
   The Policy Diagnostic page appears.

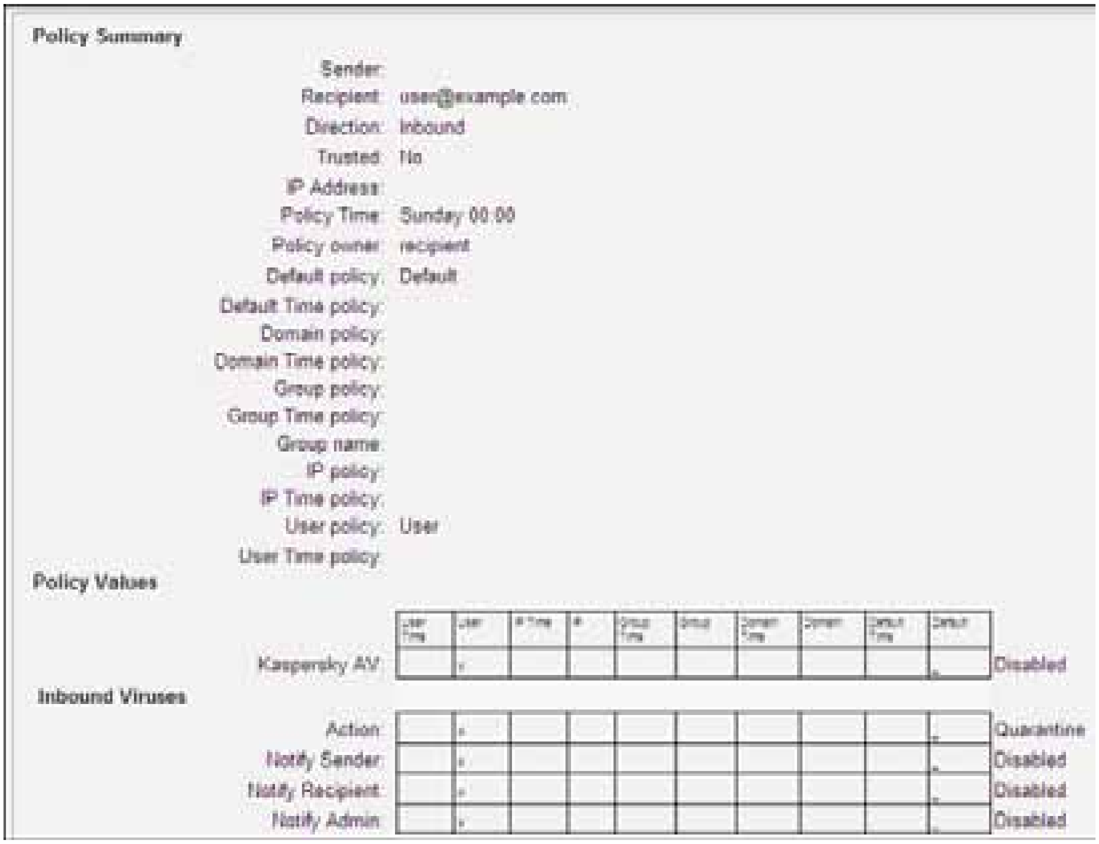


Policy Diagnostic

Sender:
Recipient: user@example.com
IP Address:
Time: Sunday 00 00
Direction: Inbound
Trusted: No

2. To test an outbound message, in the **Sender** text box, enter the test sender email address.
   Keep this field blank to indicate any sender for inbound mail.
3. In the **Recipient** text box, type the test recipient email address for the message.
   The final result displayed during the diagnostics is the final policy result for this specific user.
4. In the **IP Address** text box, type an optional IP Address for the message, if required.

5. From the **Time** drop-down list, select the time stamp for the message.
6. From the **Direction** drop-down list, select the direction for the message to determine policy results when the message is inbound or outbound.
7. From the **Trusted** drop-down list, select whether the message is considered to be from a trusted (**Yes**) or untrusted source (**No**).
8. Click **Lookup**.



Policy Summary

Sender:
Recipient: user@example.com
Direction: Inbound
Trusted: No
IP Address:
Policy Time: Sunday 00:00
Policy owner: recipient
Default policy: Default
Default Time policy:
Domain policy:
Domain Time policy:
Group policy:
Group Time policy:
Group name:
IP policy:
IP Time policy:
User policy: User
User Time policy:

Policy Values

	User Time	User	IP Time	IP	Group Time	Group	Domain Time	Domain	Default Time	Default	
Kaspersky AV:		x								_	Disabled

Inbound Viruses

Action:		x								_	Quarantine
Notify Sender:		x								_	Disabled
Notify Recipient:		x								_	Disabled
Notify Admin:		x								_	Disabled

The Policy Diagnostics summary page gives you a detailed analysis of how the various active policies combine to determine the final disposition of messages. The results include a table that displays the WatchGuard XCS features that are configured on a per-policy basis.

Each column displays the contributions to the disposition of the message by each policy (user, IP address, group, domain, and Default).

For each feature, an “X” indicates the defined policy was used to determine the final result. Any policies that were overridden by the applied policy are indicated by an “_” underscore character. An empty column indicates that a matching policy was not found by the policy resolution engine.

At the end of each feature row, the final result of the policy is indicated, for example, “Disabled” for Kaspersky Anti-Virus.

Because policies are initialized with reasonable defaults, and those values may match the overall default setting, it can appear that a particular policy has been overridden, when in fact there is no apparent configuration responsible for this. For example, the default setting for Content Scanning is “disabled”. If a user policy is defined, but Content Scanning is not part of that definition, and nothing else overrides the default, then it appears that the contribution has come from the user policy.

13 Web Scanning

About the Web Proxy

The WatchGuard XCS incorporates a Web Proxy that manages web traffic and controls access to external web sites. The system scans web traffic using a subset of the same scanners that examine email messages to inspect the content of web traffic and file transfers. With the WatchGuard XCS policy features, you can apply web access policies to different users, groups, IP addresses, and domains.

The Web Proxy analyzes client requests and allows or blocks access to specific web sites based on the configured access policies. The Web Proxy can block or allow access to web sites using Fully Qualified Domain Names (FQDN) and IP addresses, for example, http://www.example.com and http://10.1.0.10/.

Web Traffic Content Inspection

The Web Proxy inspects downloaded and uploaded content with these features:

- **Kaspersky Anti-Virus** – Scans for viruses and spyware in downloaded and uploaded files.
- **URL Block Lists** – Blocks access to web sites that appear on a URL Block List.
- **Objectionable Content Filter (OCF)** – Scans web traffic for objectionable content based on a dictionary of blocked words and phrases.
- **Attachment Control** – Allows or blocks specific file extensions and MIME types.
- **Content Scanning** – Allows or blocks files based on specific text content in a file.
- **Web Reputation** – Allows or blocks web requests based on the reputation of the web site.
- **URL Categorization** – Allows or blocks web sites based on a list of blocked web site content categories.
- **HTTP Trusted and Blocked Sites List** – Allows or blocks web sites based on a managed list of web site domains.

> ***Note*** *Content inspection is not performed on HTTPS traffic.*

Web Proxy Authentication

You can allow unauthenticated access for all users, or require authentication before access to external web sites is allowed. If authentication is enabled, all end users that use the Web Proxy must be authenticated by an LDAP server or have a local account to get access to web sites through the Web Proxy.

> ***Note*** *You cannot use local account authentication if the system is part of a cluster because local accounts are not available in a cluster.*

Users must authenticate to the system with their LDAP user ID or local account credentials and password. All access is denied until the user is authenticated to the system. If authentication is disabled, all users use the Default policy, or an IP address policy if one is assigned, for web access control. You can also configure the WatchGuard XCS to bypass HTTP authentication for specific web domains or from specific source IP addresses and networks.

Single Sign-on IP Address-based Authentication

The Web Proxy provides a way for users to log in only once to authenticate to the Web Proxy and browse web sites. The authenticated user is tracked by their IP address and users never have to re-authenticate during their browser sessions. IP-based authentication also enables authentication when using the Web Proxy in a Transparent Mode deployment.

An IP Address Portal Authentication method is also available that presents the user with a login portal page where they enter their local or LDAP user name and password and agree to a usage policy agreement before they are allowed access to browse web sites. The Portal authentication method uses HTTPS to protect the transmission of the user’s credentials.

When you use Proxy and Portal IP address-based authentication:

Users can log out of their authenticated sessions with this URL:
`http://<hostname>/portal/logout`

Users must re-authenticate to the Web Proxy if they receive a different IP address from a DHCP server when their IP address is renewed.

Make sure that no intermediary proxies are installed before the Web Proxy because clients must have a unique IP address to be identified for IP-based authentication. Clients that connect through another proxy use the IP address of the intermediary proxy server.

Traffic Accelerator

The expansive growth of large, media intensive, interactive, and collaborative web sites requires greater bandwidth that can overload corporate networks.

The WatchGuard Traffic Accelerator solution provides several web traffic enhancements to reduce bandwidth consumption, server loads, and network latency, that results in better network performance and availability. The WatchGuard Traffic Accelerator includes these features:

- **Streaming Media Bypass** – The WatchGuard Traffic Accelerator has the ability to bypass streaming media content to reduce the strain on bandwidth resources.

See *Streaming Media Bypass* for more detailed information on configuring the streaming media bypass.

- **Web Cache** – The web cache feature of the WatchGuard Traffic Accelerator solution enables faster retrieval of web sites to provide temporary storage of web data. This feature reduces bandwidth consumption and improves performance for subsequent accesses of these web sites because the data and images are read from the disk cache instead of going out to the Internet.

  See *Web Cache* for detailed information on configuring the web cache.

Web Proxy Chaining

The Web Proxy supports proxy chaining to a remote proxy server. This feature forwards requests to another proxy server in an organization’s network before it connects to the Internet. This can be a requirement in specific environments where you must access a primary proxy server before web traffic is allowed outside of the organization’s network.

> ***Note*** *TheWatchGuardXCSonlyallowsbasicauthenticationtoauthenticatetoaremote proxy.*

Automatic Client Proxy Configuration

Organizations that want to enforce the use of a proxy policy without manual configuration of each individual browser can use these methods for automatic proxy configuration:

- **Proxy Auto-Config (PAC) file** – A Proxy Auto-Config (PAC) file defines how a web browser can automatically choose an appropriate proxy server to connect to. The PAC file is a script file that browsers read and execute to determine which proxy to use.
- **Web Proxy Autodiscovery Protocol (WPAD)** – The Web Proxy Autodiscovery Protocol (WPAD) is supported by most web browsers to locate a Proxy Auto-Config (PAC) file automatically and then use this information to configure the browser's web proxy settings. The protocol can use DHCP or DNS to locate the PAC file.

Web Proxy Support and Limitations

The Web Proxy supports these types of HTTP requests:

- HTTP 1.0 and 1.1
- HTTP pipelining
- HTTP keep-alive messages

These are current limitations with the Web Proxy:

- HTTPS traffic is scanned by the proxy, but the content is not decrypted, scanned, or analyzed.
- FTP over HTTP is not supported with the Web Proxy.
- ClusteringisnotsupportedinTransparentMode.AWebProxyrunninginTransparentModecanbe clusteredwithanon-WebProxysystem,forexample,aWatchGuardXCSappliancethatprocessesemail.

Web Proxy Best Practices

These are best practices to follow when you implement the Web Proxy for the first time:

- We recommend that you run the system for at least 24-48 hours with minimal scanning enabled before you enable threat and content control scans on web traffic. This allows the web cache to be populated and increases performance. After this initial period, you can enable threat and content control scanners as needed.
- We recommend DNS caching be enabled to increase Web Proxy performance. This option is enabled by default in **Configuration > Network > Interfaces**.
- Make sure you enable **Large MTU** on the network interface designated for HTTP Proxy access. This option is enabled by default in **Configuration > Network > Interfaces**.
- When you configure the Web Proxy in Transparent Mode, make sure that you enable the **Large MTU** setting on the network interface configured as the **Bridge In** interface. You must enable the Web Proxy and reboot the system before you can enable bridging and Transparent Mode on a network interface.
- Make sure that your local DNS server is configured and works. Misconfigured DNS services and domain name translation issues can significantly decrease Web Proxy performance or cause the Web Proxy to fail.
- If you enable the URL Categorization feature, it can take several minutes to download the initial URL Categorization Control List. When the Control List is downloading, web traffic is not processed and users can receive policy error messages when web browsing. When the update is complete, web traffic processing resumes. We recommend that you do not start processing HTTP traffic until the initial download process is complete.

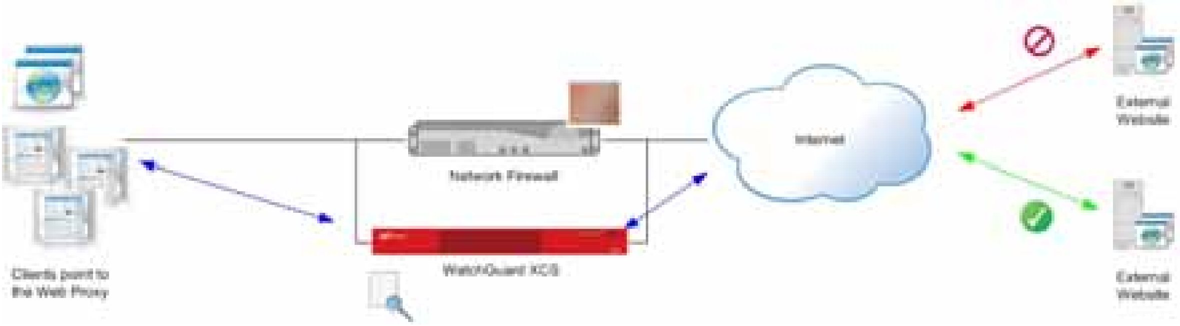
Web Deployments

You can install the Web Proxy in these types of deployments:

Full Proxy Parallel Deployment

You can deploy the Web Proxy in parallel with an existing network firewall using two network interfaces. In this configuration, you must manually configure web clients to use the WatchGuard XCS as the web proxy. You can also use proxy auto-discovery methods to automatically configure the client with the address of the XCS device. The network firewall must block HTTP traffic (for example, TCP port 80) to prevent circumvention of the proxy by network clients.

We recommend this configuration as the primary Web Proxy deployment model.



Advantages

- Requires no additional performance overhead on the Web Proxy because it only processes web traffic.
- Simple to deploy and troubleshoot connection issues.
- Appliance is located securely outside of the internal network.
- Appliance can be clustered with another WatchGuard XCS that processes web or email.
- Automated failover with no network downtime.

Disadvantages

- Must set up proxy auto-discovery using PAC Files or WPAD to point to the WatchGuard XCS.

Internal Network Deployment

You can deploy the Web Proxy on the internal network connected with one network interface. The network firewall must block HTTP traffic (for example, TCP port 80) to prevent circumvention of the proxy by network clients. HTTP port access must be allowed for the Web Proxy only.

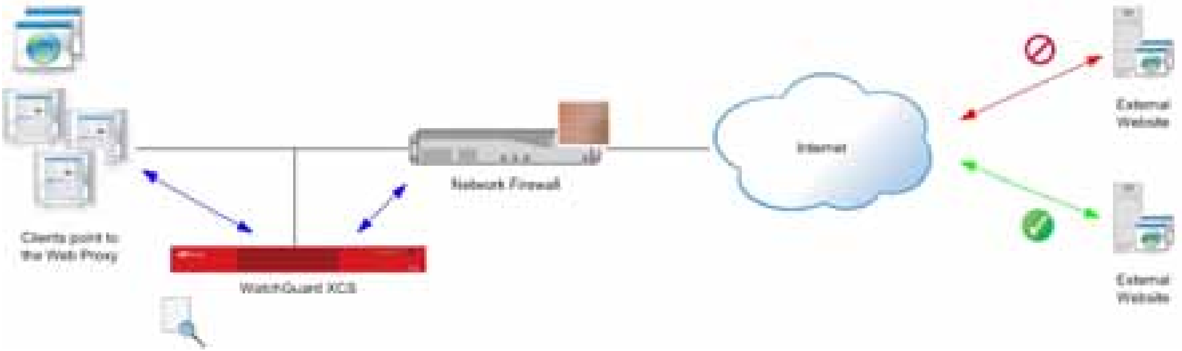
You must manually configure web clients to use the WatchGuard XCS as their web proxy. You can also use proxy auto-discovery to automatically assign the web proxy address.

Advantages

- Requires no additional performance overhead on the system.
- Simple to deploy and troubleshoot connection issues.

Disadvantages

- Must set up proxy auto-discovery using PAC Files or WPAD to point to the WatchGuard XCS.

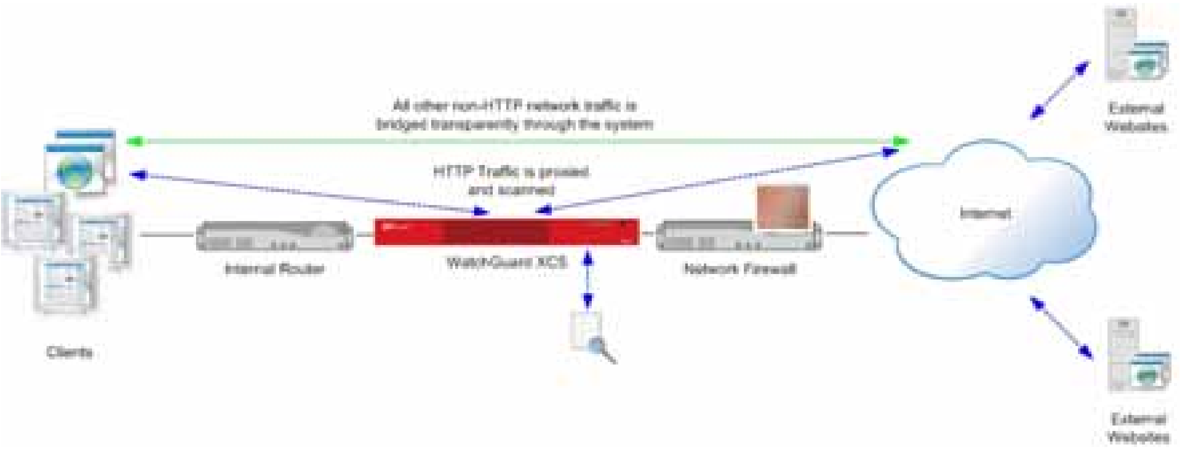


Transparent Mode Deployment

The Web Proxy offers a Transparent Mode deployment option to integrate the system into existing environments with minimal network reconfiguration. This method requires no network reconfiguration and the implementation is transparent to clients.

In a typical Transparent Mode implementation, the Web Proxy system is installed between the primary internal switch or router and an existing network firewall to act as a bridge for all non-local traffic, except selected web traffic that is examined by the Web Proxy. The system listens for web traffic on TCP port 80 and any specific HTTP requests are processed by the Web Proxy for security threat processing and content filtering before it allows the request through.

> ***Note*** *When Transparent Mode is enabled, the HTTP Proxy port must use TCP port 80.*


All other non-HTTP network traffic is bridged transparently through the system
HTTP Traffic is proxied and scanned
Clients
Internal Router
WatchGuard XCS
Network Firewall
Internet
External Websites
External Websites

You must specify two network interfaces for bridging, and the single IP address that is shared for the bridge. One of these interfaces (*Bridge In*) connects to the primary internal router or switch (LAN side), and the other interface (*Bridge Out*) connects to the network firewall.

Traffic that is bridged through the Web Proxy is not examined or modified. Traffic examined by the Web Proxy is modified to appear to originate from the local IP address of the Web Proxy. With this method, returning traffic is recognized and correctly processed for security threats and content filtering.

Advantages

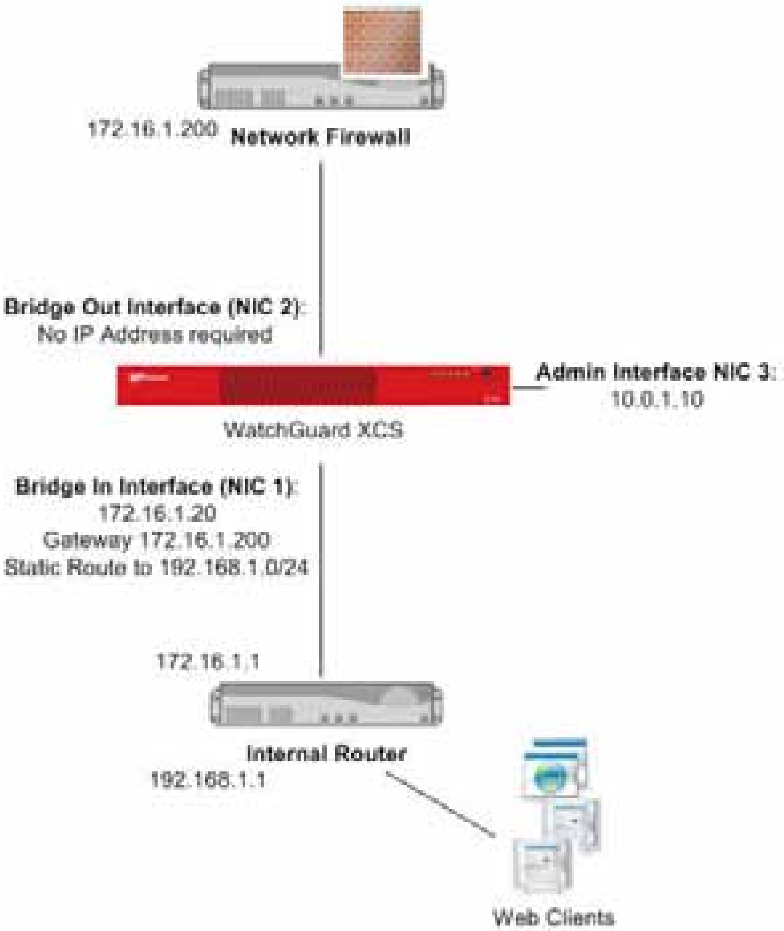
- Offers a simple and seamless deployment. No network or client system reconfiguration is required.

Disadvantages

- All network traffic is sent through the Web Proxy, which may not be preferable depending on the network environment.
- Packet inspection is performed on all traffic to determine if data should be proxied or bridged, which can add additional performance overhead on the Web Proxy.
- The default port for HTTP traffic (TCP port 80) cannot be modified in Transparent Mode.
- Only IP-based Proxy or Portal authentication can be used in Transparent Mode.
- Clustering with other Web Proxy systems is not supported in Transparent Mode. A Web Proxy that runs in Transparent Mode can be clustered with a non-Web Proxy system, for example, a WatchGuard XCS system that process email.
- If the system fails, all network traffic is stopped.

This diagram illustrates the most basic Transparent Mode implementation in which the Web Proxy is installed between the primary internal router and the network firewall.

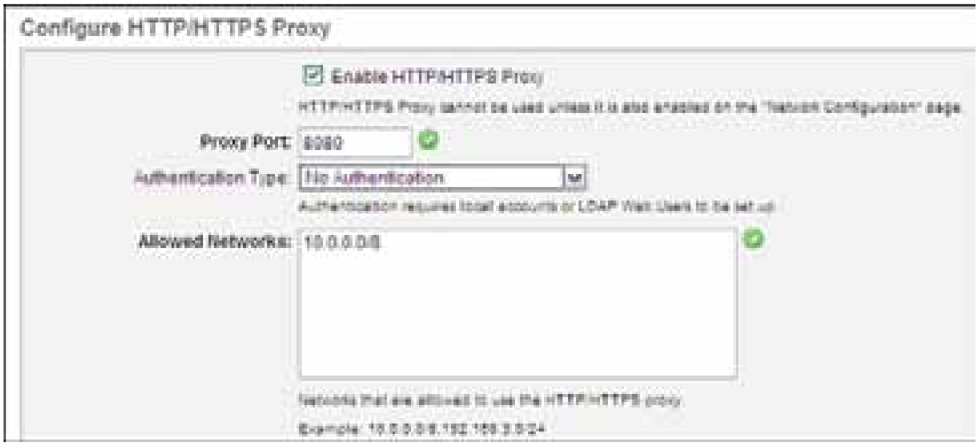
- The NIC 1 interface is designated the *Bridge In* interface and connects to the LAN side internal router. This interface must have an IP address assigned and have HTTP/HTTPS Proxy access enabled. This interface IP address is the address for the entire bridge.
- The NIC 2 interface is designated the *Bridge Out* interface and connects to the network firewall. This interface does not require any IP address configuration, and is automatically configured for use with the bridge.
- The NIC 3 interface is designated for administrative access to secure access to the system and prevent administrative access through the bridge interfaces. The *Bridge In* interface can be used for administrative access if required.
- The network gateway for the Web Proxy is the address of the network firewall.
- You must create static routes on the Web Proxy that point to your internal router networks. This is required as the web traffic uses the IP addresses on the bridge interfaces when it proxies traffic. The interface requires the network addresses to be able to route the traffic back to the internal subnetworks.



Configure the Web Proxy

To enable and configure the Web Proxy:

1. Select **Configuration > Web > HTTP/S Proxy**.



Configure HTTP/HTTPS Proxy

☑ Enable HTTP/HTTPS Proxy

HTTP/HTTPS Proxy cannot be used unless it is also enabled on the "Network Configuration" page

Proxy Port: 8080

Authentication Type: No Authentication

Authentication requires local accounts or LDAP Web Users to be set up

Allowed Networks: 10.0.0.0/8

Networks that are allowed to use the HTTP/HTTPS proxy

Example: 10.0.0.0/8,192.168.0.0/24

2. Select the **Enable HTTP/HTTPS Proxy** check box.
3. In the **Proxy Port** text box, type the port on which the Web Proxy listens for messages.
   The default is TCP port 8080. If this XCS device is deployed in Transparent Mode, the default TCP port is 80 and cannot be modified.
4. From the **Authentication Type** drop-down list, select a method of authentication.

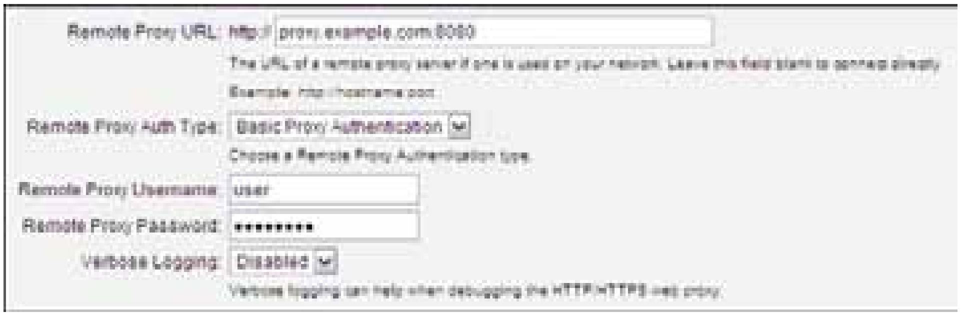
   See *Enable Web Proxy Authentication* for detailed information on configuring Web Proxy authentication.
5. In the **Allowed Networks** text box, type a comma-separated list of networks (in CIDR/slash notation format) that are allowed to get access to the Internet through the Web Proxy, for example, `10.0.0.0/8,192.168.0.0/24`

   The **Allowed Networks** text box cannot be left blank. If you want to allow all networks, type `0.0.0.0/0`.
6. In the **Remote Proxy URL** text box, type an optional address of an external proxy server to which to forward web requests.
   This is required if the WatchGuard XCS connects through an intermediary proxy server before requests are sent to the Internet.

   Type a URL with this format, hostname:port.

   For example,
   `proxy.example.com:8080`

   Keep this field blank if the system connects directly to the Internet.



Remote Proxy URL: http:// proxy.example.com:8080

The URL of a remote proxy server if one is used on your network. Leave this field blank to connect directly.

Example: http://hostname:port

Remote Proxy Auth Type: Basic Proxy Authentication

Choose a Remote Proxy Authentication type.

Remote Proxy Username: user

Remote Proxy Password: ●●●●●●●●●

Verbose Logging: Disabled

Verbose logging can help when debugging the HTTP/HTTPS web proxy.

7. If you have configured a remote proxy that requires basic authentication, from the **Remote Proxy Auth Type** drop-down list, select **Basic Proxy Authentication**.

   Type the **Remote Proxy Username** and **Remote Proxy Password** that is used to authenticate the WatchGuard XCS with the remote proxy. Make sure that you configure the specified user name on the remote proxy.

8. From the **Verbose Logging** drop-down list, select **Enabled** to turn on additional log details in the Web Proxy log.

   In the default configuration, only rejected web requests or requests that are matched in a content control feature are recorded on the *Recent Web Activity* page. To see the activity of all Web requests, including those that passed all security and content checks, enable this feature.

   > ***Warning*** *You should only enable the Verbose Logging option for a short period of time for troubleshooting purposes. Performance is negatively affected when Verbose Logging is enabled and the system is processes web requests.*

9. Click **Apply**.

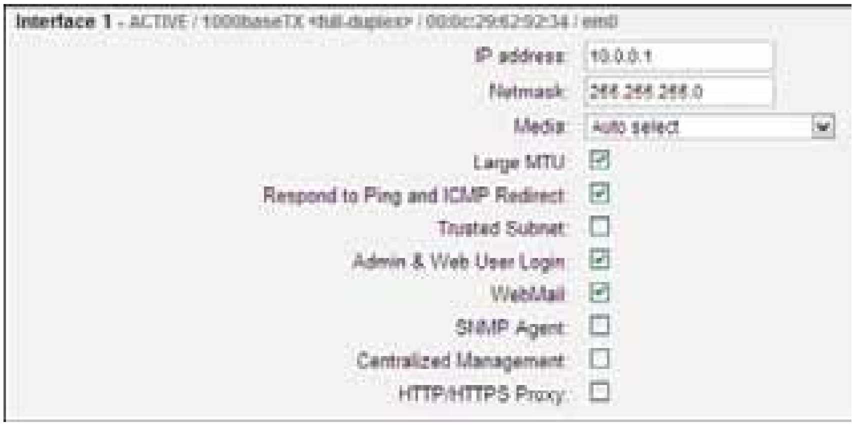
Web Proxy Network Interface Settings

You must enable Web Proxy access on a specific network interface after the Web Proxy feature is enabled globally.

> ***Note*** *You must enable the HTTP/HTTPS Proxy feature and reboot the device before you configure the network interfaces for bridging and Transparent Mode operation.*

To enable the Web Proxy on a network interface:

1. Select **Configuration > Network > Interfaces**.
2. Choose a network interface and select the **HTTP/HTTPS Proxy** check box.
3. If **IP Address Proxy** or **Portal Authentication** is enabled, make sure you enable the **Admin & Web User Login** option to allow users to authenticate through the Web Proxy.
4. If you use the Transparent Proxy feature, you must enable the **HTTP/HTTPS Proxy** and **Large MTU** check boxes and assign an IP address to the **Bridge In** interface.



Interface 1 - ACTIVE / 1000baseTX <full-duplex> / 00:0c:29:62:92:34 / em0

IP address: 10.0.0.1

Netmask: 255.255.255.0

Media: Auto select

Large MTU: ☑

Respond to Ping and ICMP Redirect: ☑

Trusted Subnet: □

Admin & Web User Login: ☑

WebMail: ☑

SNMP Agent: □

Centralized Management: □

HTTP/HTTPS Proxy: □

5. Click **Apply**.
   You must reboot the system.

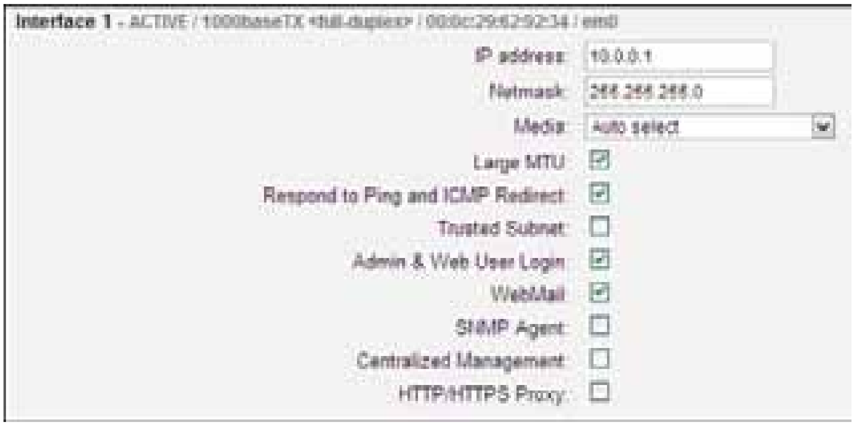
Transparent Mode

To enable the Web Proxy in Transparent Mode:

1. Select **Configuration > Web > HTTP/S Proxy**.
2. Select the **Enable HTTP/HTTPS Proxy** check box.
3. Click **Apply**.
   You must reboot the system.

> ***Note*** *You must enable the HTTP/HTTPS Proxy and reboot the device before you configure the network interfaces for Transparent Mode operation. If Transparent Mode is enabled and the HTTP/HTTPS Proxy is disabled, network traffic on TCP port 80 is blocked and the Web Proxy does not record any information. The default port for HTTP traffic (TCP port 80) cannot be modified in Transparent Mode.*

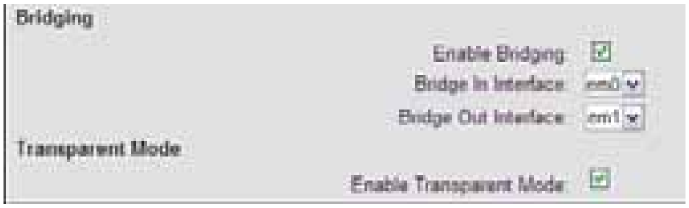
4. Select **Configuration > Network > Interfaces**.
5. Make sure that you configure the *Bridge In* network interface with an appropriate IP address.
6. Select the **HTTP/HTTPS Proxy** and **Large MTU** options.



Interface 1 - ACTIVE / 1000baseTX <full-duplex> / 00:0c:29:62:92:34 / em0

IP address: 10.0.0.1
Netmask: 255.255.255.0
Media: Auto select
Large MTU: ☑
Respond to Ping and ICMP Redirect: ☑
Trusted Subnet: □
Admin & Web User Login: ☑
WebMail: ☑
SNMP Agent: □
Centralized Management: □
HTTP/HTTPS Proxy: □

7. In the **Bridging** section, select the **Enable Bridging** check box.
   You must enable bridging for Transparent Mode to work correctly.



Bridging

Enable Bridging: ☑
Bridge In Interface: em0
Bridge Out Interface: em1

Transparent Mode

Enable Transparent Mode: ☑

8. Select a configured network interface to use as the *Bridge In* interface for Transparent Mode.

   For greater security and performance, select an interface on a dedicated, non-routable subnet. You must configure this interface with an IP address and enable the **HTTP/HTTPS Proxy** access and **Large MTU** options before you select the interface as the *Bridge In* interface.

9. Select an unconfigured network interface to use as the *Bridge Out* interface for Transparent Mode.

For greater security and performance, select an interface on a dedicated, non-routable subnet. This interface does not require an IP address and is configured automatically for use with the bridge.

10. Select the **Enable Transparent Mode** check box.
11. Click **Apply**.
    You must reboot the device.

Disable the Web Proxy in Transparent Mode

To disable the Web Proxy feature, but still allow all traffic (this includes HTTP port 80) to pass through the system while in Transparent Mode:

1. Select **Configuration > Network > Interfaces**.
2. For the **Bridge In** interface, disable the **HTTP/HTTPS Proxy** option.
3. Click **Apply**.
   You must reboot the device.

When the system restarts, all network traffic passes through the system and no Web Proxy functions are performed or recorded as log messages.

> ***Note*** *If Transparent Mode is enabled, but the HTTP/HTTPS Proxy is disabled, all TCP port 80 HTTP traffic is blocked, and no log messages for HTTP traffic are generated.*

About Web Proxy Authentication

If you enable Web Proxy authentication, users must authenticate to the WatchGuard XCS with a user name and password before they are allowed access to browse web sites.

There are two methods to configure authentication:

- **Local Account** – A local account can be set up to authenticate web users. You cannot use local account authentication if the system is part of a cluster, because local accounts are not available.

  See *Local User Accounts* for details on how to add a local user account.

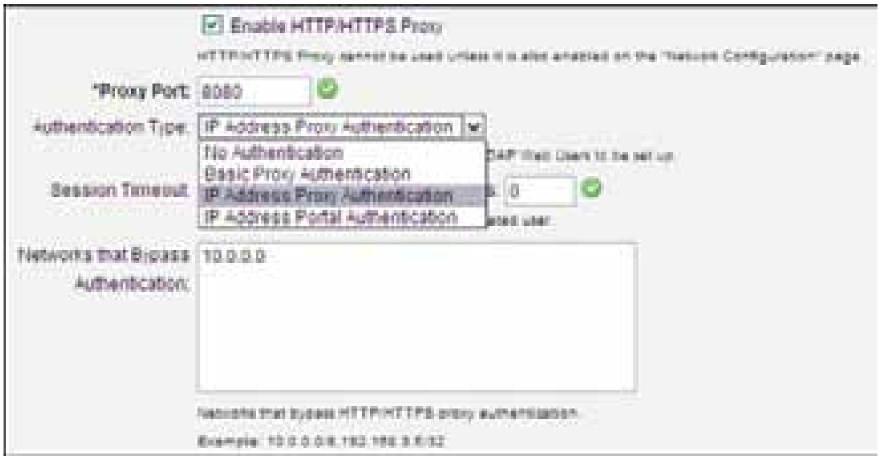
- **LDAP Web Users** – When users log in to the Web Proxy, they can be authenticated directly with an LDAP server. The LDAP Web Users feature allows LDAP-authenticated clients to use the Web Proxy feature. Web clients must use a login name and password to authenticate to an LDAP server before they can get access through the Web Proxy. LDAP Authentication enables the system to authenticate the user directly to an LDAP directory server without the need to create a local account.

  See *LDAP Web Users* for details on how to configure the LDAP Web Users feature.

Enable Web Proxy Authentication

To enable Web Proxy authentication:

1. Select **Configuration > Web > HTTP/S Proxy**.
   The Configure HTTP/HTTPS Proxy page appears.



☑ Enable HTTP/HTTPS Proxy

HTTP/HTTPS Proxy cannot be used unless it is also enabled on the "Network Configuration" page

*Proxy Port: 8080

Authentication Type: IP Address Proxy Authentication

Session Timeout: 0

Networks that Bypass Authentication: 10.0.0.0

Networks that bypass HTTP/HTTPS proxy authentication.

Example: 10.0.0.0/8,192.168.3.6/32

No Authentication
Basic Proxy Authentication
IP Address Proxy Authentication
IP Address Portal Authentication

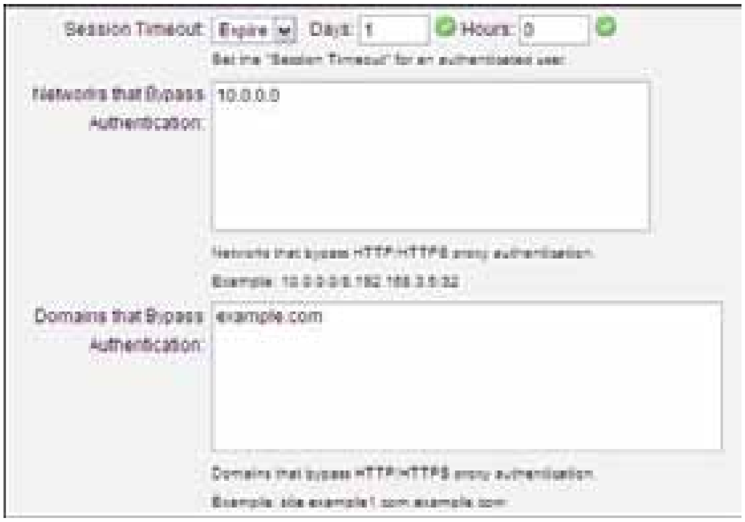
2. From the **Authentication Type** drop-down list, select the authentication method.

   - **No Authentication** – Disables authentication and allows all users access to web sites through the Web Proxy. If **No Authentication** is selected, web clients always use the Default policy settings, or an IP address policy if one is assigned, for web access.
   - **Basic Authentication** – Allows only authenticated users access to web sites through the Web Proxy. The user must have a local account or must be authenticated directly to an LDAP server. The user must log in with their local or LDAP user name and password before they can connect to web sites through the Web Proxy. When you use Basic Authentication, the user's credentials are sent in clear text. The user must enter their credentials for each browser session.
     Basic Authentication mode is not supported when you use the Web Proxy in Transparent Mode.
   - **IP Address Proxy Authentication** – Allows only authenticated users access to web sites through the Web Proxy. The user must have a local account or must be authenticated directly to an LDAP server. The user must log in with their local or LDAP user name and password before they can connect to web sites through the Web Proxy. When you use the Proxy Authentication method, the user's credentials are sent as basic HTTP authentication in clear text. The system tracks the user based on their IP address. The user is never prompted again for their credentials in any current or new web browser session. IP address proxy authentication mode is supported when you use the Web Proxy in full proxy mode and Transparent Mode.
   - **IP Address Portal Authentication** – Allows only authenticated users access to web sites through the Web Proxy. Users are presented with a web proxy login portal page where they must enter their local or LDAP user name and password, and agree to a usage policy agreement before they are allowed access to browse web sites. (You can customize the usage policy agreement on the **Configuration > Miscellaneous > Customization** page.) The Portal Authentication method uses HTTPS to protect the transmission of the user's credentials. The system tracks the user with their IP address. The user is never prompted again for their credentials in any current or new web browser session. IP address portal authentication mode is supported when you use the Web Proxy in full proxy mode and Transparent Mode.

> ***Note*** *If you use the IP Address-based Proxy and Portal Authentication methods, you must enable the* ***Admin & Web User Login*** *option on the HTTP Proxy network interface*

> *for users to authenticate to the Web Proxy. If you use IP address-based authentication in full proxy mode, there is additional configuration required on the client browser to route authentication requests correctly. See Web Client Configuration for details.*

3. These options appear when you select any of the authentication options:



Session Timeout: Expire Days: 1 Hours: 0

Set the "Session Timeout" for an authenticated user.

Networks that Bypass Authentication: 10.0.0.0

Networks that bypass HTTP/HTTPS proxy authentication.

Example: 10.0.0.0/8,192.168.3.5/32

Domains that Bypass Authentication: example.com

Domains that bypass HTTP/HTTPS proxy authentication.

Example: site.example1.com,example.com

- **Session Timeout** – When you use IP Address Proxy or Portal Authentication mode, you can set a session expiry timeout that forces the user to re-authenticate when they exceed the time out value.
  - **Never** – The user session never expires. This setting is persistent if the system restarts.
  - **Expire** – The user session expires after the specified time period (in days and hours). The user is required to re-authenticate when their session expires.
- **Networks that Bypass Authentication** – Type a comma-separated list of networks that bypass authentication. Any user on these networks is not required to authenticate to use the Web Proxy.
- **Domains that Bypass Authentication** – Type a comma-separated list of domains that bypass authentication. If a user gets access to the specified web domain, they are not required to authenticate to the Web Proxy. All subdomains of the specified domain are included.

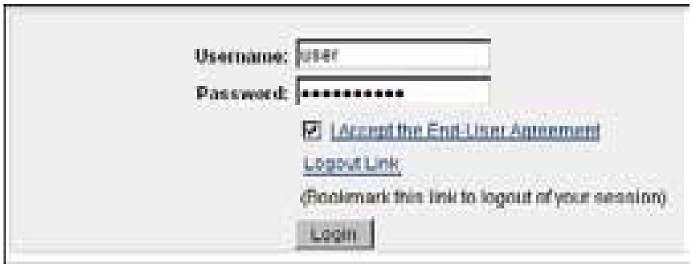
  Authentication bypass occurs before policy resolution. Users that bypass authentication always use the Default policy, or an IP address policy if one is assigned, for their access settings. Any web requests to a domain that bypasses authentication are not reported in the user's web reporting information because only the IP address is recorded.

Web Proxy Authentication Logout

Web Proxy Portal and Proxy authenticated users have the ability to log out of their sessions. This is useful for shared computers that are used by several different users to make that each user uses their own Web Proxy policies when they browse web sites.

When the user logs in to the Web Proxy Portal Authentication page, a URL is displayed that redirects the user to the portal logout page where "<my_hostname>" is the address of the WatchGuard XCS. We recommend the user bookmarks this URL in their client web browser.

```
http://<my_hostname>/portal/logout
```



Username: user

Password: ••••••••••

☑ I Accept the End-User Agreement

Logout Link

(Bookmark this link to logout of your session)

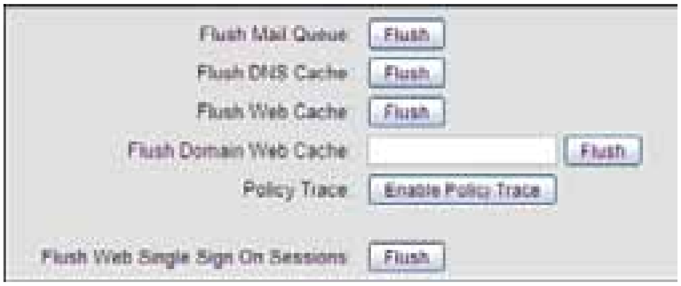
For Proxy authenticated users that do not use the Portal, you must provide this URL to the end users.

Flush All Web Single Sign-on Sessions

To force a logout of all Portal and Proxy IP address-based authenticated users, you can flush all authenticated sessions from the **Activity > Status > Utilities** page. Web Proxy users must re-authenticate before they can get access to web sites through the Web Proxy.

> ***Note*** *In a cluster, the Flush button is available only on the Primary cluster system.*

1. Select **Activity > Status > Utilities**.



2. In the **Flush Web Single Sign-On Sessions** section, click the **Flush** button.

   The system flushes all Web Proxy authenticated sessions for both Proxy and Portal IP address-based authenticated users.

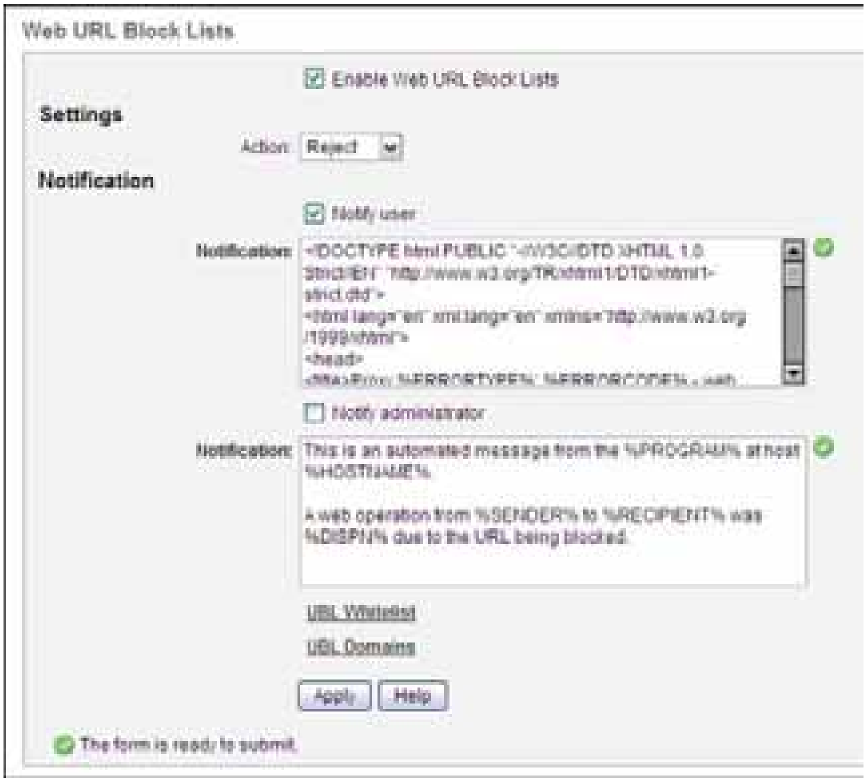
Web URL Block Lists

URL Block Lists contain a list of domains and IP addresses of URLs that have appeared previously in spam, phishing, or other malicious web site content.

The URL Block Lists feature allows you to block access to web site URLs that appear on a URL Block List.

To enable URL Block Lists:

1. Select **Configuration > Web > URL Block Lists**.
   The Web URL Block Lists page appears.



Web URL Block Lists

☑ Enable Web URL Block Lists

Settings

Action: Reject

Notification

☑ Notify user

Notification:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0
Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-
strict.dtd">
<html lang="en" xml:lang="en" xmlns="http://www.w3.org
/1999/xhtml">
<head>
<title>Proxy: %ERRORTYPE% %ERRORCODE% - web
```

□ Notify administrator

Notification:

```
This is an automated message from the %PROGRAM% at host
%HOSTNAME%.

A web operation from %SENDER% to %RECIPIENT% was
%DISPN% due to the URL being blocked.
```

The form is ready to submit.

2. Select the **Enable Web URL Block Lists** check box.
3. From the **Action** drop-down list, select an action to take if a URL is on a URL Block List.
4. Select **Reject** to reject the web request.
5. Select **Just Log** to allow the request and record the event in the Web Proxy log.
6. Select **Notify user** to enable notification to the end user if the web site is blocked.
   You can customize the notification sent to the end user.
7. Select **Notify administrator** to enable notification to the administrator if the web site is blocked.
   You can customize the notification sent to the administrator.

> ***Note*** *Notifications are not sent for a Just Log action.*

8. Select **UBL Whitelist** to configure domains that bypass URL Block List processing.
9. Select **UBL Domains** to customize the URL Block List lookup domains to use for URL checks.
10. Click **Apply**.

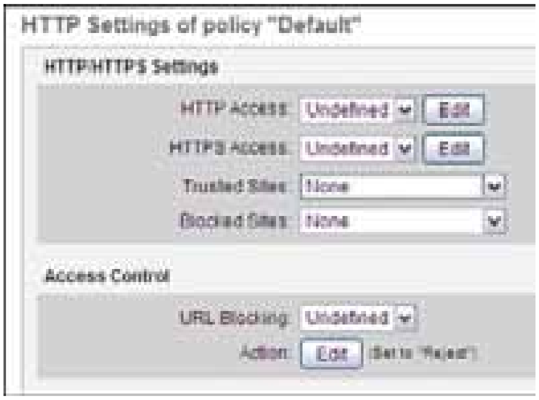
Configure URL Block Lists in a Policy

The *URL Blocking* option uses the URL Block List feature to block access to specific web sites.

To enable URL Blocking in a policy:

1. Select **Configuration > Web > More > URL Block Lists**.
2. Select the **Enable Web URL Block Lists** check box.
3. Click **Apply**.
4. Select **Security > Policies > Policies**.

5. Select an existing policy to configure its settings, or create a new policy.
6. Select **HTTP**.



HTTP Settings of policy "Default"

HTTP/HTTPS Settings

HTTP Access: Undefined Edit

HTTPS Access: Undefined Edit

Trusted Sites: None

Blocked Sites: None

Access Control

URL Blocking: Undefined

Action: Edit (Set to "Reject")

7. From the **URL Blocking** drop-down list, select **Enabled**, or select **Undefined** to use the inherited settings from another overriding policy or the Default policy.
8. Click **Edit** to set the **Action** to either **Reject** to reject the connection (default), or **Just Log** to allow the connection and record the issue in the Web Proxy log.
9. You can enable and configure notifications for the administrator and end user.

   You can customize the notification only in the Default policy. Notifications are only sent for a **Reject** action, not **Just Log**.

10. Click **Apply**.

Web Reputation

The Reputation Enabled Defense (RED) service helps to identify web sites that contain malicious or inappropriate content. It reports behavioral information based on a collection of statistics about a web site URL. The statistics are based on the occurrences of the web site hosting viruses, spyware, and malware. This information is collected from installed WatchGuard products worldwide that share their Web Anti-Virus and Spyware scanning results with RED.

The Web Reputation feature queries the RED service for the reputation of the requested web site URL. With this information, the WatchGuard XCS can make a decision about whether to allow or block a web site request based on the reputation score of the web site URL.

Reputation Score

The reputation score can be from 1 to 100. A reputation closer to 1 is good and indicates the web site is extremely reliable and rarely hosts viruses or spyware. A reputation closer to100 is bad and indicates the web site is extremely unreliable and often spreads viruses and spyware. A web site with no previous information from any source is assigned an initial neutral value of 50.

You can set a reputation threshold over which web URLs are rejected. For example, if you set the threshold to 90, any web URL with a reputation score greater than 90 is rejected. This prevents your web clients from access to URLs that have historically hosted viruses and spyware.

The reputation score is tracked for a specific URL path, for example, *www.example.com/url/path*. The corresponding top-level domain reputation, *example.com*, is independently tracked, and the amount of web site URLs with a good reputation at that top-level domain reflects positively on its reputation, even if a sub-domain or hosted URL contains viruses or spyware and has a bad reputation. For example, a URL that hosts a virus at *www.example.com/url/path/virus.exe* can have a reputation of 98, but the top-level domain site *www.example.com* can have reputation score of 55.

Web Reputation Statistics Sharing

When you enable Web Reputation, web scanning statistics from your device are shared with the Reputation Enabled Defense service. This information is collected from installed WatchGuard products worldwide to generate the reputation score for web sites based on Anti-Virus and Spyware scanning results (Clean, Virus-infected, Spyware-infected, and Suspicious).

> ***Note*** *Web Reputation queries and statistics sharing uploads to RED use UDP port 10108. This port must be opened up on your network firewall if the WatchGuard XCS is located behind the firewall.*

Bypass Anti-Virus and Spyware Scanning

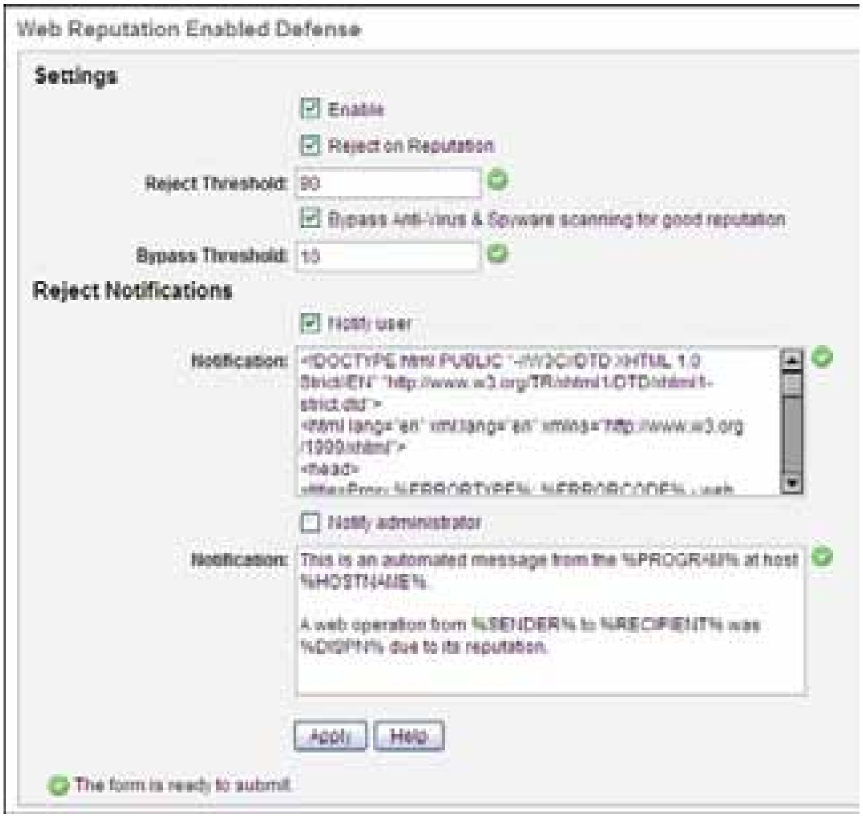
You can bypass Anti-Virus and Spyware scanning for web requests if the reputation of the requested web site URL is below a specified bypass threshold. For example, if you set the bypass threshold to 10, any web site with a reputation score lower than 10 bypasses Anti-Virus and Spyware scanning.

This feature increases the performance of web processing because the WatchGuard XCS must do only minimal scanning for web sites with good reputations where the probability of harmful content is minimal.

Configure Web Reputation

To configure Web Reputation:

1. Select **Configuration > Web > Reputation Enabled Defense**.
2. To enable Web Reputation lookups and allow statistics to be shared with RED, select the **Enable** check box.



Web Reputation Enabled Defense

Settings

☑ Enable

☑ Reject on Reputation

Reject Threshold: 90

☑ Bypass Anti-Virus & Spyware scanning for good reputation

Bypass Threshold: 10

Reject Notifications

☑ Notify user

Notification:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0
Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-
strict.dtd">
<html lang="en" xml:lang="en" xmlns="http://www.w3.org
/1999/xhtml">
<head>
<title>Proxy: %ERRORTYPE% %ERRORCODE% - web
```

□ Notify administrator

Notification:

```
This is an automated message from the %PROGRAM% at host
%HOSTNAME%.

A web operation from %SENDER% to %RECIPIENT% was
%DISPN% due to its reputation.
```

The form is ready to submit.

3. Select the **Reject on Reputation** check box to enable reputation lookups for web URLs to the RED network.
4. In the **Reject Threshold** text box, type a threshold over which a web site is blocked. You must enter a value between 1 and 100. The default value is 90. If the reputation of a web site is greater than this value, the web request is rejected. The lower the reputation threshold, the greater the chance you could block a legitimate web site.
5. In the **Bypass Scanning** section, select the **Bypass Anti-Virus & Spyware scanning for good reputation** check box to bypass Anti-Virus scanning for web requests if the reputation of the requested web site URL is below the specified threshold.

   This feature increases the performance of web processing because the XCS device does only minimal scanning for web sites with good reputations where the probability of harmful content is minimal.
6. In the **Bypass Threshold** text box, type the threshold below which web sites bypass Anti-Virus scanning.

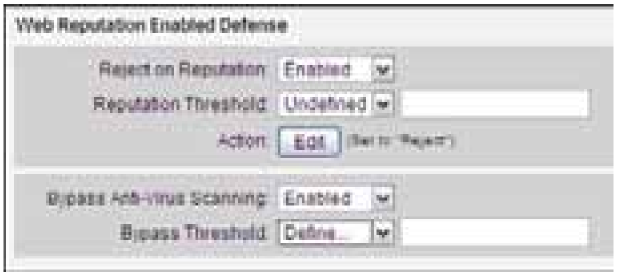
   You must enter a value between 1 and 100. The default is 10. The higher the bypass threshold, the greater the chance you could bypass Anti-Virus and Spyware scanning for a malicious web site.
7. Select **Notify user** to send a notification to the end user if the web site is blocked.
   You can customize the notification sent to the end user.
8. Select **Notify administrator** to send a notification to the administrator if the web site is blocked.
   You can customize the notification sent to the administrator.
9. Click **Apply**.

Configure Web Reputation in a Policy

The Web Reputation feature queries the RED service for the reputation score of the requested web site URL. With the information returned from RED, the WatchGuard XCS can make a decision about whether to allow or block a web site request based on the reputation of the web site.

To configure Web Reputation settings in a policy:

1. Select **Configuration > Web > Reputation Enabled Defense**.
2. Select the **Enable** check box.
3. Click **Apply**.
4. Select **Security > Policies > Policies**.
5. Select a policy to configure, or create a new policy.
6. In the policy editor, select the **HTTP** section.
7. In the **Web Reputation Enabled Defense** section, enable or disable **Reject on Reputation** for this policy.
   Select "Undefined" to use the inherited value from another policy, the Default policy, or the global settings.



Web Reputation Enabled Defense

Reject on Reputation: Enabled

Reputation Threshold: Undefined

Action: Edit (Set to "Reject")

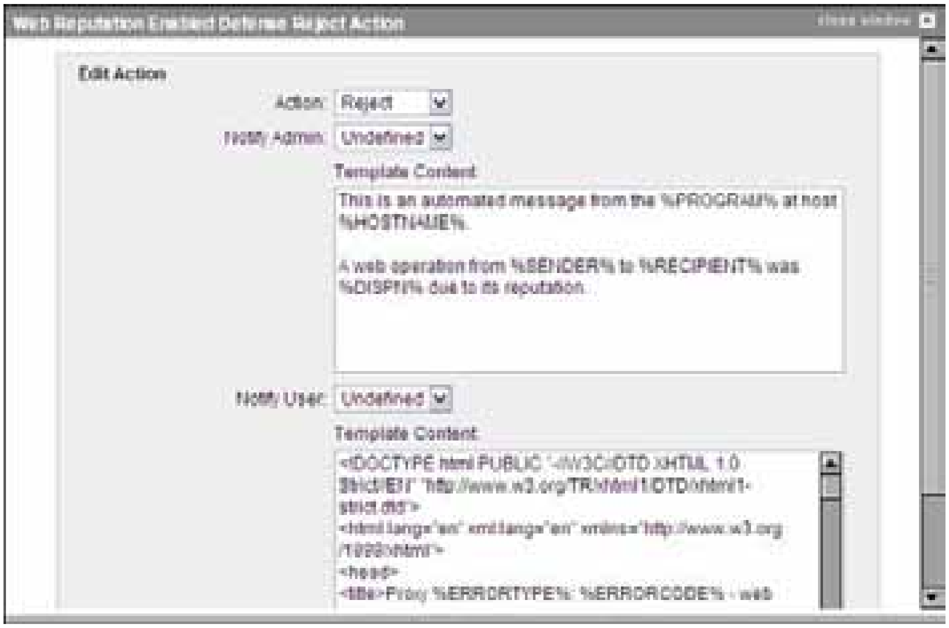
Bypass Anti-Virus Scanning: Enabled

Bypass Threshold: Define...

8. From the **Reputation Threshold** drop-down list, select **Define** to enter a value.
   Select "Undefined" to use the inherited value from another policy, the Default policy, or the global settings.

   Type a reputation threshold score over which a web site is blocked. If the reputation score of a web site is greater than this value, it is blocked. Note that the lower the reputation threshold, the greater the chance that a valid web site is blocked.

9. In the **Action** field, click **Edit** to define an action to take if a web site reputation score exceeds the configured **Reputation Threshold**.



Edit Action

Action: Reject

Notify Admin: Undefined

Template Content

This is an automated message from the %PROGRAM% at host %HOSTNAME%.

A web operation from %SENDER% to %RECIPIENT% was %DISP[illegible]% due to its reputation.

Notify User: Undefined

Template Content

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0
Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-
strict.dtd">
<html lang="en" xml:lang="en" xmlns="http://www.w3.org
/1999/xhtml">
<head>
<title>Proxy %ERRORTYPE%: %ERRORCODE% - web
```

- **Reject** – Rejects the web request and prevents clients from access to the web site.
- **Just Log** – Web sites that exceed the Reputation Threshold are recorded in the Web Proxy log file, but no action is taken on the web site URL and the web connection is not blocked.

You can enable and configure notifications for the administrator and end user when a web site is blocked because of a bad reputation. You can customize the notification only in the Default policy.

Notifications are only sent for a **Reject** action, not **Just Log**.

10. From the **Bypass Anti-Virus Scanning**, drop-down list, enable or disable the option to bypass Anti-Virus scans for web connections if the reputation score of the requested web site is below the specified threshold.

    This feature increases the performance of web processing because the XCS device does only minimal scans for web sites with good reputations where the probability of harmful content is minimal.

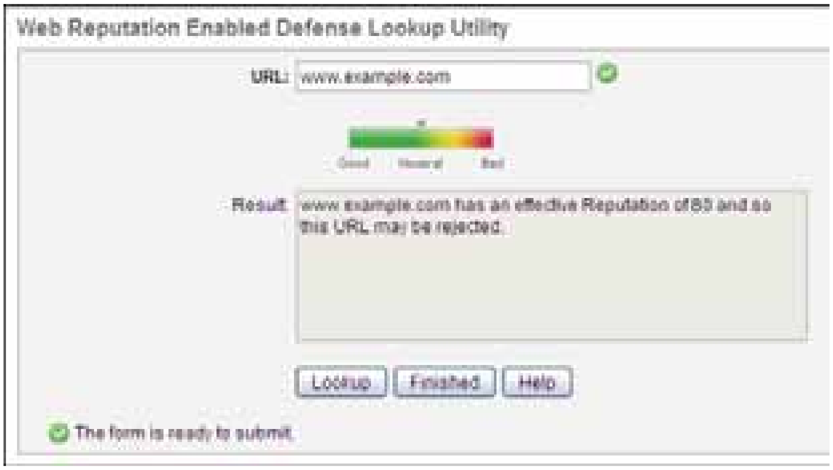
11. From the **Bypass Threshold** drop-down list, select **Define** and type a threshold below which web sites bypass Anti-Virus scanning.
    Select "Undefined" to use the inherited value from another policy, the Default policy, or the global settings.
12. Click **Apply**.

Web Reputation Lookup

You can enter a web site URL to check its current reputation score.

To check the reputation of a web site URL:

1. Select **Activity > Status > Utilities**.
2. In the **Diagnostics** section, click **Web RED Lookup**.



Web Reputation Enabled Defense Lookup Utility

URL: www.example.com

Result: www.example.com has an effective Reputation of 83 and so this URL may be rejected.

The form is ready to submit.

3. Enter a web URL address.
   You do not have to enter the prefix http://.

   For example, `www.example.com`
4. Click **Lookup**.
   The results of the reputation lookup appear.

   A reputation closer to 1 indicates the web site is extremely reliable and rarely hosts viruses or spyware. A reputation closer to 100 indicates the web site is extremely unreliable and often spreads viruses and spyware. A web site with no previous information from any source is assigned an initial neutral value of 50.

   The top-level domain receives an independent reputation of any URL it hosts, and its overall reputation score is continually adjusted based on the amount of URLs it hosts with good and bad reputations.

Traffic Accelerator

The WatchGuard Traffic Accelerator solution provides several web traffic enhancements to reduce bandwidth consumption, server loads, and network latency, which results in better network performance and availability.
The WatchGuard XCS TrafficAccelerator includes these features:

- **Streaming Media Bypass** – To manage streaming media traffic, the WatchGuard Traffic Accelerator can bypass streaming media content to reduce the strain on bandwidth resources.
- **Web Cache** – The web cache feature of the WatchGuard Traffic Accelerator solution enables faster retrieval of web sites because it provides temporary storage of web data. This feature reduces bandwidth consumption and improves performance for subsequent accesses of these web sites because the data and images are read from the disk cache instead of going out to the Internet.

Web Cache

The Web Proxy uses a disk cache that caches data and images from web sites visited by users of the Web Proxy. This feature reduces bandwidth consumption and improves performance for subsequent accesses of these web sites because the data and images are read from the disk cache instead of going out to the Internet to retrieve the data.

The web request is compared to the cached data of the requested web site to make sure it has the latest data to update the disk cache with any web site updates. Any access of cached data is still sent to the Web Proxy content scanners because different users can have different HTTP content policies applied to them.

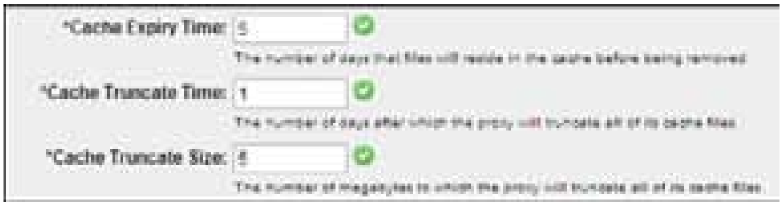
> **Note** *We recommend that you run the system for at least 24-48 hours with minimal scanning enabled before you enable Anti-Virus and deep content scans on HTTP traffic. This populates the web cache and increases performance when for access to web content. After this initial period, enable Anti-Virus and content control scanners with policies.*

All file types are cached depending on the web server HTTP directive that identifies what files are allowed to be cached. For example, HTTP redirects and cookies are not cached for security reasons. There is no limit to the size of a file that can be cached.

By default, the web disk cache is purged every 5 days, which removes any files that are older than 5 days. Data in the cache older than 1 day is truncated to less than 5MB in size for each cached domain to make sure that cached data does not take up a large amount of disk space. These default values make sure that the cache size does not grow too large and affect system performance.

To configure the advanced Web Proxy cache settings:

1. Select **Configuration > Web > Traffic Accelerator**.
2. Go to the cache settings section.



*Cache Expiry Time: 5
The number of days that files will reside in the cache before being removed

*Cache Truncate Time: 1
The number of days after which the proxy will truncate all of its cache files

*Cache Truncate Size: 5
The number of megabytes to which the proxy will truncate all of its cache files

- **Cache Expiry Time** – Indicates how long (in days) files reside in the web cache before they are expired and purged. The default is 5 days, which indicates that files older than 5 days are removed from the cache.
- **Cache Truncate Time**– Indicates the period (in days) after which data in the web cache is truncated based on the value specified in the **Cache Truncate Size** option. The default is 1 day.
- **Cache Truncate Size** – Indicates the size threshold (in MB) to which data in the web cache is truncated for each cached domain. The default is 5 MB.

3. Click **Apply**

> **Note** *These settings are advanced options and must only be modified with guidance from Technical Support. Misconfiguration can negatively affect performance.*

Web Cache Disk Use

The web disk cache is located in the local mail storage area. To see the details of this disk partition:

1. Select **Activity > Status > Utilities**.
2. In the **Disk Usage** section, the **Mail Storage Area** indicates the percentage of disk space used and the space available in the web disk cache. If you store local mailboxes on the server, this partition also includes stored local mail.

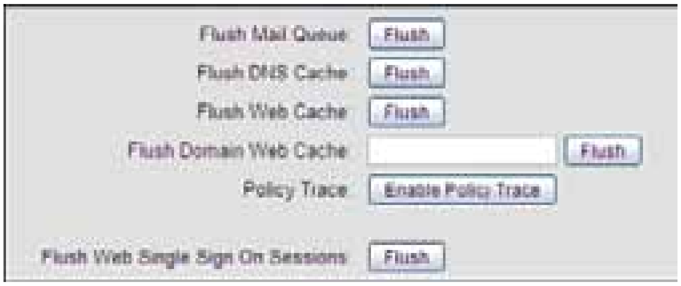
Flush the Web Cache

By default, the WatchGuard XCS is set to automatically purge the web cache every 5 days to remove all files that are older than 5 days. You can configure this option on the **Configuration > Web > Traffic Accelerator** page.

On the **Activity > Status > Utilities** page, you can manually purge the web cache. You may want to purge the entire web cache to resolve issues with certain web pages that do not updated with newer content, or problems with connections to specific web sites.

To flush the web cache:

1. Select **Activity > Status > Utilities.**
2. Go to the **Utilities** section.
3. Adjacent to **Flush Web Cache**, click **Flush**.
   This action completely empties the web cache and restarts the Web Proxy service.



Flush Web Cache Domains

You can also flush the Web Cache for only a specific domain. The URL must be specified exactly how it is typed when you browse to it, for example, www.example.com, or news.example.com. Subdomains are not included and must be flushed separately.

To flush the cache entries for a specific domain:

1. Select **Activity > Status > Utilities**.
2. In the **Flush Domain Web Cache** text box, type the required domain, for example, `www.example.com`.
3. Click **Flush**.
   Only cached entries for the www.example.com domain are purged from the web cache.

Streaming Media Bypass

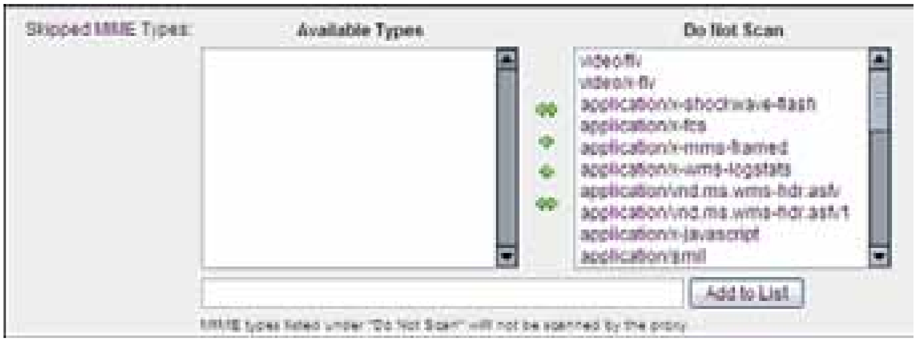
The Web Proxy can proxy and scan embedded streaming media content to provide quick delivery of data to the requesting web client.

You can configure a list of specific MIME content types that bypass Web Proxy threat and content control scanners and are delivered immediately to the web client. A predefined default list of common streaming media types is configured to bypass scanners. When you skip a streaming media type, all scanners (Anti-Virus, the Objectionable Content Filter, Content Scanning, and Attachment Control) are bypassed.

Configure Skipped MIME types

To modify the list of MIME types that bypass content and threat scanning:

1. Select **Configuration > Web > Traffic Accelerator**.



MIME types listed under "Do Not Scan" will not be scanned by the proxy

2. Use the arrow icons to add or remove items from the **Available Types** and **Do Not Scan list**.
3. You can add a new MIME type if it is not in the current list.

   Type a valid MIME time in the texts box, for example, `video/x-flv` for Flash video, and then click **Add to List**

   The new type is immediately added to the Do Not Scan section.

4. Click **Apply**.

These are the default MIME types that bypass scanners:

MIME Type	Description
application/smil	Synchronized Multimedia Integration Language
application/vnd.ms.wms-hdr.asfv	Windows Media
application/vnd.ms.wms-hdr.asfv1	Windows Media
application/x-fcs	Flash Communication Server
application/x-javascript	Javascript
application/x-mms-framed	Windows Media
application/x-quicktimeplayer	Quicktime Player

MIME Type	Description
application/x-quicktime-response	Quicktime Player response
application/x-shockwave-flash	Shockwave Flash
application/x-wms-logstats	Windows Media
audio/mp4	MP4 Audio
audio/mpeg	MP3 or other MPEG audio
audio/x-scpls	Shoutcast Playlist
image/x-icon	Website favicon format
video/flv	Flash video
video/m4v	Video (Protected)
video/mp4	MP4 video
video/mpeg	MPEG-1 video
video/quicktime	QuickTime video
video/vnd.mpegurl	M4U format
video/x-dv	Digital Video File
video/x-flv	Flash Video
video/x-m4v	Video (Protected)
video/x-ms-asf	Windows Media
video/x-msvideo	Video for Windows (AVI)
video/x-ms-wmv	Windows Media Video
video/x-sgi-movie	SGI Movie

Web Client Configuration

Depending on the deployment configuration, web clients must have their web browser proxy set to the address of the WatchGuard XCS, for example, *hostname.example.com:8080*.

The disadvantage of this method is that it is not scalable for large user environments in which manual browser reconfiguration is not practical. You can also implement proxy auto-discovery or traffic redirection methods that use additional routers or traffic managers.

To avoid the need for manual web browser configuration, we recommend that you use the Transparent Mode deployment. See *Transparent Mode* for more details on the Transparent Mode deployment.

To manually set a proxy server setting in Internet Explorer 7:

1. Select **Tools > Internet Options**.
2. Select the **Connections** tab.

3. Click **LAN Settings**.
4. In the **Proxy server** section, type the hostname or IP address of the proxy, for example, `hostname.example.com`, and set the port used by the proxy, for example, `8080`.

To manually set a proxy server setting in Mozilla Firefox 3:

1. Select **Tools > Options**.
2. Click **Advanced**.
3. Select the **Network** tab.
4. Click **Settings**.
5. In the **Manual Proxy Configuration** section, type the hostname or IP address of the proxy, for this example, `hostname.example.com`, and set the port used by the proxy, for this example, `8080`.

Optionally, if your organization uses an automatic proxy configuration, you can configure your web client to detect automatic proxy settings.

IP Authentication Browser Configuration Mode

If you use IP address-based authentication in Web Proxy mode (not in Transparent Mode), the client web browser tries to route the authentication request and response through the proxy itself. This can cause a proxy loop because the proxy server uses its own IP address instead of the client. An error is displayed in the web browser that prevents authentication to the proxy server.

To prevent this issue, you must configure the client browser to bypass the local proxy server address.

> ***Note*** *This browser configuration change is not required when using IP-based authentication in Transparent Mode.*

To bypass the proxy server address in Internet Explorer 7:

1. Select **Tools > Internet Options**.
2. Select the **Connections** tab.
3. Click the **LAN Settings**.
4. Click **Advanced**.
5. In the **Exceptions** section, type the address of the proxy server, for example, `192.168.1.200`.

   You can also add a network wildcard, for example, `192*`.

To bypass the proxy server address in Mozilla Firefox 3:

1. Select **Tools > Options**.
2. Click **Advanced**.
3. Select the **Network** tab.
4. Click **Settings**.
5. In the **No Proxy for:** section, type the address of the proxy server, for example, `192.168.1.200`.

   You can also add a network, for example, `192.168.1.0/24`.

Automatic Web Proxy Client Configuration

Organizations that want to enforce the use of a proxy policy do not want to manually configure each individual browser can use these methods for automatic proxy configuration:

- **Proxy Auto-Config (PAC) file** — A Proxy Auto-Config (PAC) file defines how a web browser can automatically choose an appropriate proxy server to connect to. The PAC file is a script file that browsers read and execute to determine which proxy to use.
- **Web Proxy Autodiscovery Protocol (WPAD)** — The Web Proxy Autodiscovery Protocol (WPAD) is supported by most web browsers to automatically locate a Proxy Auto-Config (PAC) file, and then use this information to configure the browser's web proxy settings. The protocol can use DHCP or DNS to locate the PAC file.

PAC File

You can use a PAC file with a web browser's proxy settings to configure the browser with the proxy server address. The PAC file can be hosted locally or on a network server. If you use the PAC file with WPAD, the file must be called "wpad.dat".

A simple PAC file contains text that sets the address for the proxy. For example,

```
function FindProxyForURL(url, host){return "PROXY proxy.example.com:8080";}
```

You can create more advanced proxy configurations.

For example,

```
function FindProxyForURL(url, host)
{   if (isInNet(host, "192.168.1.0", "255.255.255.0")) {
      return "DIRECT";   }
   else if (url.substring(0, 5) == "http:") {
         return "PROXY 192.168.1.200:8080";   }
   else if (url.substring(0, 6) == "https:") {
         return "PROXY 192.168.1.200:8080";   }
   else {      return "DIRECT";   }
}
```

In this example, 192.168.1.0 is the local network you want to bypass, and 192.168.1.200 is the address of the proxy server. You can also use a fully qualified domain name (FQDN), for example, *proxy.example.com*.

Replace these example addresses with your local network and proxy server addresses. If the server fails to respond, then the browser tries to contact the web server directly and does not use the proxy server.

Load Balance on IP Address

This example assigns even and odd IP addresses to different proxy servers to distribute web proxy connections:

```
function FindProxyForURL(url, host)
{
        var ipSubs = myIpAddress().split(".");
        if ( (ipSubs[3] % 2) == 0 ) {
                return "PROXY 192.168.1.200:8080 ; PROXY 192.168.1.201:8080";
        } else  {
                return "PROXY 192.168.1.201:8080 ; PROXY 192.168.1.200:8080";   }
}
```

Load Balance on URL Address

This example assigns requested URL addresses to specific proxy servers based on the letters in the URL to distribute web proxy connections:

```
function FindProxyForURL(url, host)
{       ret = URLhash(url);
        if ( (ret % 2) == 0 ){
                return "PROXY 192.168.1.200:8080 ; PROXY 192.168.1.201:8080";
        } else  {
                return "PROXY 192.168.1.201:8080 ; PROXY 192.168.1.200:8080";
        }
}function URLhash(name){var  cnt=0;
        var str=name.toLowerCase(name);
        if ( str.length ==0) {
                return cnt;
}
for(var i=0;i >= str.length ; i++) {
           var ch= atoi(str.substring(i,i + 1));
                cnt = cnt + ch;
}
        return cnt ;
}
function atoi(charstring)
{

if ( charstring == "a" ) return 0x61; if ( charstring == "b" ) return 0x62;
if ( charstring == "c" ) return 0x63;  if ( charstring == "d" ) return 0x64;
if ( charstring == "e" ) return 0x65;  if ( charstring == "f" ) return 0x66;
if ( charstring == "g" ) return 0x67;  if ( charstring == "h" ) return 0x68;
if ( charstring == "i" ) return 0x69;  if ( charstring == "j" ) return 0x6a;
if ( charstring == "k" ) return 0x6b;  if ( charstring == "l" ) return 0x6c;
if ( charstring == "m" ) return 0x6d;  if ( charstring == "n" ) return 0x6e;
if ( charstring == "o" ) return 0x6f;  if ( charstring == "p" ) return 0x70;
if ( charstring == "q" ) return 0x71;  if ( charstring == "r" ) return 0x72;
if ( charstring == "s" ) return 0x73;  if ( charstring == "t" ) return 0x74;
if ( charstring == "u" ) return 0x75;  if ( charstring == "v" ) return 0x76;
if ( charstring == "w" ) return 0x77;  if ( charstring == "x" ) return 0x78;
if ( charstring == "y" ) return 0x79;  if ( charstring == "z" ) return 0x7a;
if ( charstring == "0" ) return 0x30;  if ( charstring == "1" ) return 0x31;
if ( charstring == "2" ) return 0x32;  if ( charstring == "3" ) return 0x33;
if ( charstring == "4" ) return 0x34;  if ( charstring == "5" ) return 0x35;
if ( charstring == "6" ) return 0x36;  if ( charstring == "7" ) return 0x37;
if ( charstring == "8" ) return 0x38;  if ( charstring == "9" ) return 0x39;
if ( charstring == "." ) return 0x2e;
return 0x20;
}
```

Bypass the Proxy for Specific URLs and Domains

You can specify URLs and entire web domains to bypass the proxy, for example, local Intranet traffic or problematic web sites, in the PAC file. The specific PAC file entries for the URLs and domains must be inserted before the proxy server specification in the PAC file.

```
function FindProxyForURL(url, host)
{
// our local URLs from the domains below example.com don't need a proxy:
      if (shExpMatch(url,"*.example.com/*"))                 {return "DIRECT";}
      if (shExpMatch(url, "*.example.com:*/*"))              {return "DIRECT";}
      return "PROXY 10.1.77.200:8080; DIRECT";
}
```

WPAD with DNS

The DNS-based WPAD mechanism builds a series of URLs that point to a wpad.dat PAC file. The series of URLs starts with the full primary domain name and continues to progressively shorter suffixes until the base domain is used. For example, if the full primary domain name is host.country.example.com, the URLs attempted are:

```
http://wpad.country.example.com/wpad.dat
http://wpad.example.com./wpad.dat
```

If the web browser is configured to automatically detect proxy settings, it tries to download the PAC file from each URL until it either succeeds or runs out of URLs to check. If the client cannot connect to any of the URLs, then the web browser tries to contact the web server directly and does not use the proxy server.

WPAD with DHCP

The DHCP-based WPAD mechanism passes the URL of the PAC file as option number 252 in the DHCP lease granted to the system. If the web browser is configured to automatically detect proxy settings, it gets the URL from the DHCP lease to download the PAC file. The DHCP Server must be configured to use option 252 (that contains the URL of PAC file) in the DHCP lease.

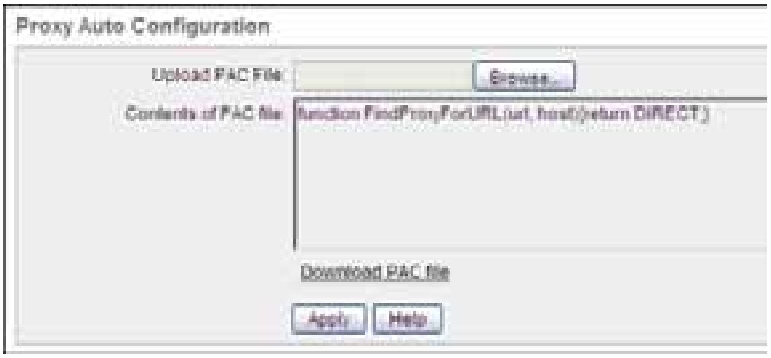
Web Proxy Auto Configuration

You can upload a PAC file that client web browsers can use with WPAD or manual configuration to retrieve the PAC file settings.

> ***Note*** *PAC files are not replicated in a cluster or in Centralized Management. In a cluster environment, only one system in the cluster must be used to host the PAC file.*

To upload a PAC file to the WatchGuard XCS:

1. Select **Configuration > Web > Proxy Auto Configuration**.



Contents of PAC file: function FindProxyForURL(url, host){return DIRECT;}

2. Click **Browse** to select a file.
   This file must be a text file. The file can have any name, but it is made available to web clients as wpad.dat.
3. Click **Apply**.
   The contents of the PAC file appear.
4. Configure the web browser clients to use WPAD automatic settings, or with the URL to the WatchGuard XCS PAC file.

   For example:
   `http://proxy.example.com/wpad.dat`

Internet Explorer Client Configuration

To configure proxy server settings in Internet Explorer 7:

1. Select **Tools > Internet Options**.
2. Select the **Connections** tab.
3. Click **LAN Settings**.
4. Select one of these options:

   - **To use WPAD to automatically detect the proxy settings for the network:**
     Select **Automatically detect settings**. The web browser uses WPAD methods to discover the

location of the configuration file with DNS or DHCP.

- **To manually enter the script path:**
  Select the **Use automatic configuration script** check box and enter the location of the PAC file. The PAC file can be stored locally or at a network URL.
  For example,
  `http://proxy.example.com/wpad.dat`

Mozilla Firefox Client Configuration

To configure proxy server settings in Mozilla Firefox 3:

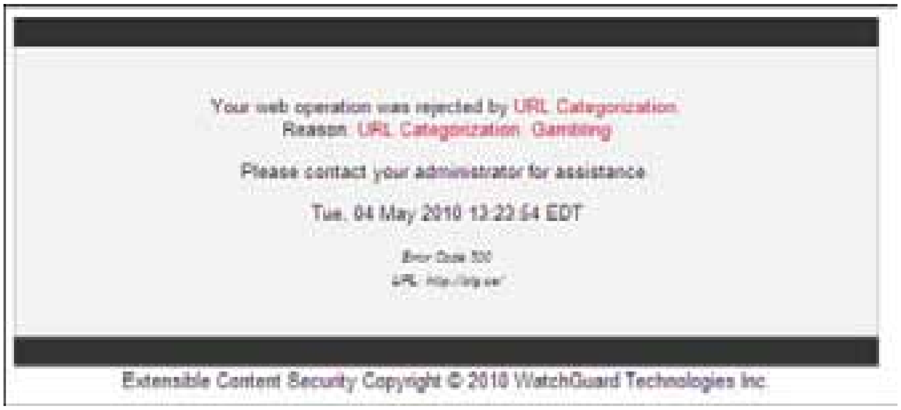
1. Select **Tools** > **Options**.
2. Select **Advanced**.
3. Select the **Network** tab.
4. Click **Settings**.
5. Select one of these options:

- **To use WPAD to automatically detect the proxy settings for the network:**
  Select **Auto-detect proxy settings for this network**. The web browser uses WPAD methods to discover the location of the configuration file with DNS or DHCP.
- **To manually enter the URL for the configuration:**
  Select the **Automatic proxy configuration URL** option and enter the location of the PAC file. The PAC file can be stored locally or at a network URL.
  For example:
  `http://proxy.example.com/wpad.dat`

Client Browser Notifications

If a web request is blocked by any security or content scanning feature, the web client displays an error notification.

For example,



Your web operation was rejected by URL Categorization
Reason: URL Categorization: Gambling

Please contact your administrator for assistance

Tue, 04 May 2010 13:22:54 EDT

Error Code 500
URL: http://[illegible]

Extensible Content Security Copyright © 2010 WatchGuard Technologies Inc

The error message shows the reason why the web request is rejected. In this example, the web request is blocked because the web site is in a blocked URL Categorization category.

You can customize the HTTP notifications in policies in the Default policy.

Web Proxy Access with Policies

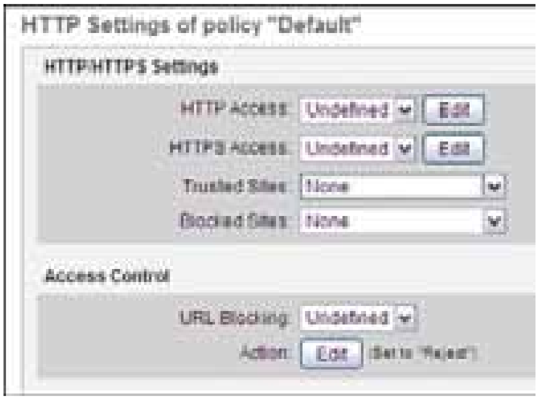
The Web Proxy uses policies to define access and content controls for different users, groups, IP addresses, and domains.

> **Note** *When you modify an HTTP policy, it can take up to two minutes for the policy change to take effect because the Web Proxy service must be restarted. Any current web sessions, for example, streaming media and logged-in web sessions, are reset.*

To configure the Web Proxy settings in a policy:

1. Select **Security > Policies > Policies**.
2. Select a policy to configure, or create a new policy.
3. In the policy editor, select the **HTTP** section.
4. From the **HTTP Access** and **HTTPS Access** drop-down lists, select **Enabled** or **Disabled**, or set to **Undefined** to use the settings inherited from another policy, the Default policy, or the global settings.

   If these options are “Undefined”, they inherit the state of the global setting for the HTTP Proxy (enabled or disabled).

   HTTP Settings of policy "Default"

   HTTP/HTTPS Settings

   HTTP Access: Undefined

   HTTPS Access: Undefined

   Trusted Sites: None

   Blocked Sites: None

   Access Control

   URL Blocking: Undefined

   Action: (Set to "Reject")

5. Click **Apply**.

Web Policy Scanner Actions

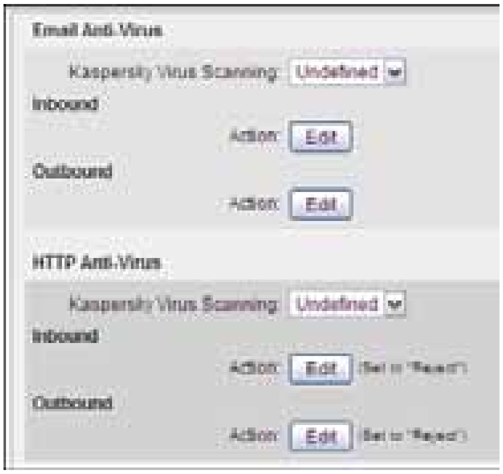
For each feature that scans web traffic, you can set a configurable action. These scanners include inbound and outbound Anti-Virus and Spyware scanning, Attachment Control, Content Scanning, and the Objectionable Content Filter (OCF).

> **Note** *If you use Attachment Control with Web content and set a “Reject” HTTP action for blocked image types and other web file types, this action effectively stops many web sites from working correctly because files required to see the web site are blocked.*

To configure the Web Proxy actions in a policy:

1. Select **Security > Policies > Policies**.
2. Select a policy to configure, or create a new policy.
3. In the policy editor, select the **Anti-Spam and Anti-Virus** section (for Anti-Spam, Anti-Virus, and Spyware), or the **Content Control** section (for Attachment Control, Content Scanning, and OCF).

   In this example, you can select actions for inbound and outbound Anti-Virus for HTTP.



Email Anti-Virus

Kaspersky Virus Scanning: Undefined

Inbound

Action: Edit

Outbound

Action: Edit

HTTP Anti-Virus

Kaspersky Virus Scanning: Undefined

Inbound

Action: Edit (Set to "Reject")

Outbound

Action: Edit (Set to "Reject")

4. In the **Action** field, click **Edit** to define an action to take:

   - **Reject** – Rejects the web request and prevents clients from access to the web site.
   - **Just Log** – Web sites are recorded in the Web Proxy log file, but no action is taken and the web connection is not blocked.

   You can enable and configure notifications for the administrator and end user when a web site is blocked. You can customize the notification only in the Default policy.

   Notifications are only sent for a **Reject** action, not **Just Log**.

HTTP Trusted and Blocked Sites

The *Trusted Sites* list allows the administrator to upload a list of web sites that bypass all scanning features. This includes Anti-Virus, HTTP content control (Attachment Control, Objectionable Content, Content Scanning), and URL filtering features (URL Blocking and URL Categorization).

The *Blocked Sites* list contains a list of domains and IP addresses that are blocked to end users that access these sites through the Web Proxy.

> ***Note*** *If a site appears in both the Trusted and Blocked Sites list, the Trusted Sites list takes precedence.*
> *Any web sites defined in the HTTP Trusted or Blocked Sites list override the URL Categorization block list.*

Create a Trusted or Blocked Sites List

To create a list of domains for a Trusted or Blocked Sites list:

1. Create a list of domains and IP addresses in a text file. Use one domain per line.

   For example,

   `example.comexample2.com192.168.1.128`

   All subdomains of the specified domain are included. For example, the domain `example.com` includes `subdomain.example.com`.
2. Select **Security > Content Control > Dictionaries & Lists**.
3. Click **Add**.
4. Browse and locate your list of trusted or blocked sites, then click **Continue**.
   The first few lines of the list appear.
5. Set the list **Type** to **Domain** to indicate this is a list of domains and IP addresses.
   The "Any" list type can also be specified.
6. Click **Continue**.
   The details of the uploaded file appear.
7. Click **Continue**.
   The final details of the uploaded list appear.
8. Confirm the details, and make sure the list type is set to **Domain** or **Any**.
9. Click **Save**.

   In the HTTP policy, you can now select the list as a Trusted or Blocked Sites list.

Configure Trusted and Blocked Sites Lists

To configure the HTTP Trusted and Blocked Sites lists:

1. Select **Security > Policies > Policies**.
2. Select an existing policy, or create a new policy.
3. Select **HTTP**.
4. Set **Trusted Sites** to **None** to make sure that all web sites browsed through the Web Proxy are scanned by the Web Proxy's scan features, or select a predefined list of **Trusted Sites** from the drop-down list.

   This list of web sites bypass all HTTP scans for users of the Web Proxy.
5. Set **Blocked Sites** to **None** to not block any specific web sites, or select a predefined list of **Blocked Sites** from the drop-down list.

   These sites are blocked and Web Proxy users cannot get access to this sites.

Web Proxy URL and IP Address Blocking

The Web Proxy does not do PTR (Pointer record) reverse lookups for each site browsed to, and when you block a specific hostname, it does not block the associated IP address for that hostname if it is specified. You must add the IP address separately to a block list to prevent access to the web site with its IP address.

For example, if you want to block www.example.com, you must make sure you block both the domain name www.example.com, and its corresponding IP address, for example, 192.168.1.128.

If you enter an IP address, it blocks both the IP and domain name if the domain name resolves to that same address.

If you use an address list with the Trusted and Blocked Sites feature, you can add domain names and IP addresses to the same list using a **Domain** or **Any** type list.

For example,

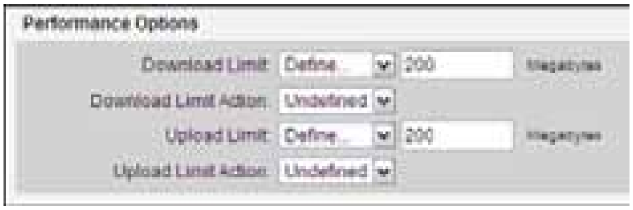
```
example.com192.168.1.128website.com10.10.1.10
```

HTTP Upload and Download Limit

In the HTTP section of a policy, you can set a limit on the size of both HTTP uploads and downloads to prevent unnecessary load on network and system resources. When a file exceeds the specified threshold, the file can be blocked, or scanning can be bypassed to allow the upload and download of large files without the use of a large amount of system scanning resources.

To configure HTTP upload and download limits:

1. Select **Security > Policies > Policies**.
2. Select an existing policy or create a new policy.
3. Select **HTTP**.
4. In the **Performance Options** section, type the largest size (in MB) allowed for an HTTP upload or download.
   The default is 7 MB. Leave the field defined as blank or “0” for no limit. Select **Undefined** to use the inherited settings from another overriding policy or the Default policy.



Performance Options

Download Limit: Define... 200 Megabytes

Download Limit Action: Undefined

Upload Limit: Define... 200 Megabytes

Upload Limit Action: Undefined

5. Set the **Download Limit Action** and **Upload Limit Action** that is applied when the file exceeds the size threshold:

   - **Undefined** – Any limits and actions on downloads and uploads use the inherited settings from another overriding policy or the Default policy.
   - **Block** – The file transfer is blocked, and an error message is sent to the web client to indicate the reason the download or upload was blocked.
   - **Bypass** – The file transfer is not blocked and bypasses any HTTP content scans. This allows the upload and download of larger files and prevents them the use of too many scan resources because of their size. This is the default value.

URL Categorization

URL Categorization is a licensed option you can use together with the Web Proxy. This feature prevents HTTP access to web sites based on a predefined Control List of blocked web sites organized in several topic categories. Because it transparently blocks undesirable Internet content, URL Categorization can assist in productivity management and reduce network bandwidth consumed by Internet browsing.

Web site filtering prevents clients in an organization from connections to non-business related web sites, provides protection against malicious web sites, prevents viruses and malware from entering an organization, and prevents users from visits phishing sites.

URL Categorization uses a single global Control List database of millions of web sites classified into over 50 categories from hundreds of countries and in over 65 languages. The list of web sites and their categories is continuously updated, and updates to the Control List database are downloaded daily by the XCS system.

URL Categorization filters web sites based on the Fully Qualified Domain Name (FQDN), for example, *www.example.com*. You can block or allow any specific category of web sites. You can also configure URL Categorization and category selection with policies, and specify a list of web sites that are not categorized so they are not blocked by URL Categorization.

> ***Note*** *Any web sites defined in the HTTP Trusted or Blocked Sites list (configured in policies) override URL Categorization blocking.*

These are the default web site categories for URL Categorization:

URL Categorization Categories	
Adult/Sexually Explicit	Kids Sites
Advertisements & Popups	Motor Vehicles
Alcohol & Tobacco	News
Arts	Peer-to-Peer
Blogs & Forums	Personals & Dating
Business	Philanthropic & Professional Orgs.
Chat	Phishing & Fraud
Computing & Internet	Photo Searches
Criminal Activity	Politics
Downloads	Proxies & Translators
Education	Real Estate
Entertainment	Reference
Fashion & Beauty	Religion
Finance & Investment	Ringtones/Mobile Phone Downloads
Food & Dining	Search Engines
Gambling	Sex Education
Games	Shopping
Government	Society & Culture
Hacking	Spam URLs

URL Categorization Categories	
Health & Medicine	Sports
Hobbies & Recreation	Spyware
Hosting Sites	Streaming Media
Illegal Drugs	Tasteless & Offensive
Infrastructure	Travel
Intimate Apparel & Swimwear	Violence
Intolerance & Hate	Weapons
Job Search & Career Development	Web-based Email

Default Blocked Categories

These web site categories typically contain inappropriate and offensive content, and are blocked by default:

Default Blocked Categories	
Adult/Sexually Explicit	Phishing & Fraud
Alcohol & Tobacco	Spam URLs
Criminal Activity	Spyware
Gambling	Tasteless & Offensive
Hacking	Violence
Illegal Drugs	Weapons
Intolerance & Hate	

Categories to Block if Required by an Organization

These additional web site categories could be blocked based on the requirements of an organization. These categories include blogs, games, webmail, and streaming media sites.

Categories to Block if Required by an Organization	
Advertisements & Pop-Ups	Personals and Dating
Blogs & Forums	Photo Searches
Chat	Proxies & Translators
Downloads	Ringtones/Mobile Phone Downloads
Games	Sex Education
Hosting Sites	Sports
Intimate Apparel & Swimwear	Streaming Media

Categories to Block if Required by an Organization	
Job Search & Career Development	Travel
Peer-to-Peer	Web-based Email

Categories to Block to Enhance Productivity

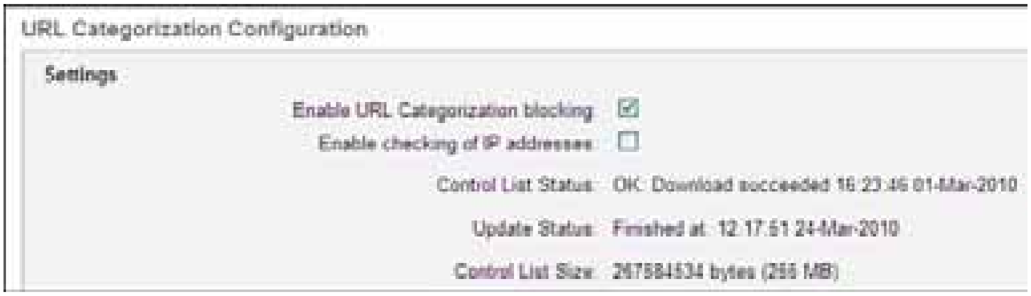
These web site categories can be blocked to increase productivity in an organization, if required. These categories include news, entertainment, and shopping web sites.

Categories to Block to Enhance Productivity	
Computing & Internet	Kid's Sites
Business	Motor Vehicles
Computing & Internet	News
Education	Philanthropic & Professional Orgs.
Entertainment	Politics
Fashion & Beauty	Real Estate
Finance & Investment	Reference
Food & Dining	Religion
Government	Search Engines
Health & Medicine	Shopping
Hobbies & Recreation	Society & Culture
Infrastructure	

Configure URL Categorization

To configure URL Categorization:

1. Select **Configuration > Web > URL Categorization**.



URL Categorization Configuration

Settings

Enable URL Categorization blocking ☑

Enable checking of IP addresses □

Control List Status: OK: Download succeeded 16:23:46 01-Mar-2010

Update Status: Finished at: 12:17:51 24-Mar-2010

Control List Size: 267584534 bytes (255 MB)

2. Select the **Enable URL Categorization blocking** check box.

URL Categorization immediately starts to download the latest Control List database. A download status appears in the **Control List Status** section.

The Control List is very large, and it can take several minutes for the list to download the first time. While the Control List downloads, HTTP messages are not processed, and users can receive policy error messages. When the update is complete, HTTP message processing resumes.We recommend that you do not start processing HTTP messages until this initial download process is complete.

In a cluster, the Control List is not replicated from a cluster Primary to Secondary systems. To update the Control List on the Secondary, change the run mode to Standalone, update the Control List, and switch back to Secondary mode.

3. Select the **Enable checking of IP addresses** check box (enabled by default) to check the resolved IP addresses of URLs against the URL Categorization Control List.

   If you enable IP address checking, legitimate URLs can be blocked by URL Categorization because they originate from a shared IP address where other blocked sites also originate. A best effort is made to resolve the IP address of the URL, however, IP address blocking may not immediately take effect for an URL the first time it is browsed to because the address may not have been immediately resolved before the request was processed.

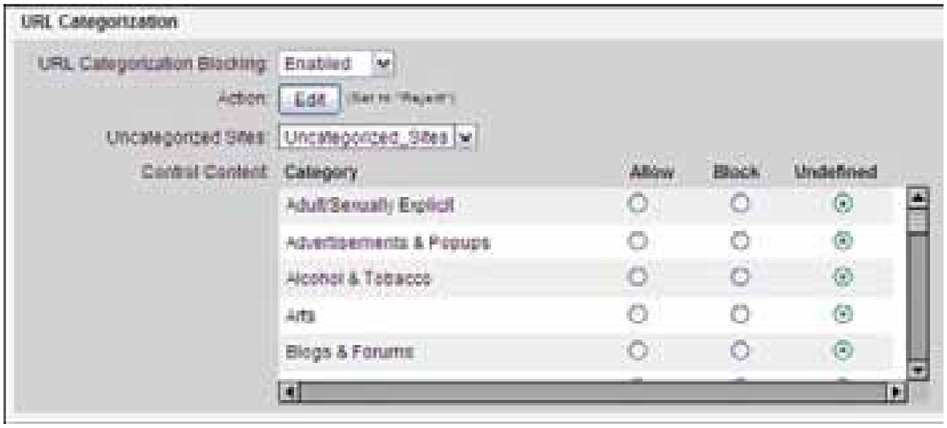
   For each category, select the corresponding option to enable blocking of the web sites in that category, or clear the check box to allow clients to connect to the web sites in that category.
4. Click **Apply**.

Configure URL Categorization in a Policy

You can customize URL Categorization blocking and the Control List categories to use when you create access control policies.

To configure URL Categorization settings in a policy:

1. Select **Configuration > Web > URL Categorization**.
2. Select the **Enable URL Categorization blocking** check box.
3. Click **Apply**.
4. Select **Security > Policies > Policies**.
5. Select which policy to configure, or create a new policy.
6. In the policy editor, select the **HTTP** section.
7. In the **URL Categorization** section, enable or disable URL Categorization blocking for this policy, and select which categories are allowed or blocked.
   Select "Undefined" to use the inherited value from another policy, the Default policy, or the global settings.



URL Categorization

URL Categorization Blocking: Enabled

Action: Edit (Set to "Reject")

Uncategorized Sites: Uncategorized_Sites

Control Content:

Category	Allow	Block	Undefined
Adult/Sexually Explicit	○	○	●
Advertisements & Popups	○	○	●
Alcohol & Tobacco	○	○	●
Arts	○	○	●
Blogs & Forums	○	○	●

8. Click **Edit** to modify the HTTP action of the message if the URL is blocked by URL Categorization.

   - **Reject** – Rejects the web request and prevents clients from access to the web site.
   - **Just Log** – Categorized web sites are recorded in the Web Proxy log file, but no action is taken on the web site URL and the web connection is not blocked.

   You can enable and configure notifications for the administrator and end user when a web site is blocked because of URL Categorization. You can customize the notification only in the Default policy.

   Notifications are only sent for a **Reject** action, not **Just Log**.

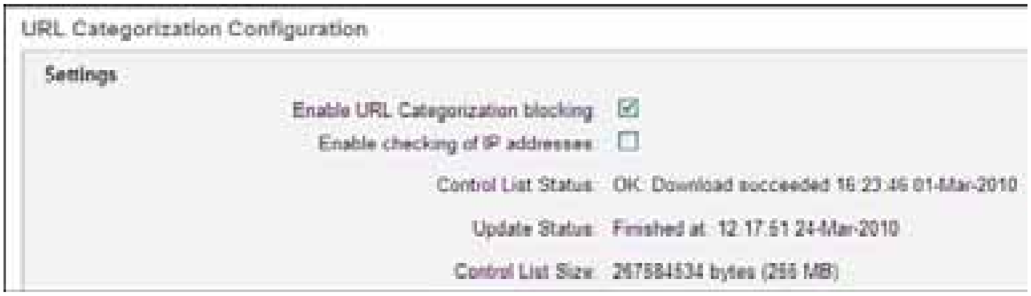
9. From the **Uncategorized Sites** drop-down list, select a list that contains the web site domains that are exempt from categorization by the URL Categorization feature.

Control List Updates

Click **Update Control List** to manually download and apply the latest URL Categorization Control List.

The **Control List Status** section displays the date of the latest Control List download. Updates to the Control List are automatically downloaded every 24 hours at 12:00 AM. Control List database updates are incremental and only take a short amount of time to complete after the initial Control List download.

URL Categorization uses TCP port 80 to download the Control List. This port must be open for the WatchGuard XCS if the device is located behind a network firewall.



URL Categorization Configuration

Settings

Enable URL Categorization blocking ☑

Enable checking of IP addresses □

Control List Status: OK: Download succeeded 16:23:46 01-Mar-2010

Update Status: Finished at: 12:17:51 24-Mar-2010

Control List Size: 267584534 bytes (255 MB)

The status of the download can be seen from **Activity > Logs > System**.

For example,

```
May 22 13:21:16 host spl: sc_download=started 16-May-2008May 22 13:21:16 host spl:
sc_download=Download in progress
```

The Control List is very large, and it can take several minutes for it to download the first time. While the Control List downloads, HTTP messages are not processed and users can receive policy error messages. When the update is complete, HTTP message processing resumes. Further Control List updates are incremental and only take a short amount of time to complete.

Uncategorized Sites

The *Uncategorized Sites* feature enables you to create a list of web site domains that are exempt from URL Categorization. This enables you to create a whitelist of specific web sites to make sure they are not blocked by URL Categorization.

To create a list of web site domains:

1. Create a list of domains and IP addresses in a text file, with one domain per line.

   For example,

   ```
   example.com
   example2.com
   example3.com
   192.168.1.10
   ```

   All subdomains of the specified domain are included. The domain `example.com` also includes `subdomain.example.com`.
2. Select **Security > Content Control > Dictionaries & Lists**.
3. Click **Add**.
4. Browse and locate your list of web site domains, then click **Continue**.
   The first few lines of the list appear.
5. Set the list **Type** to **Domain** to indicate this is a list of domains and IP addresses.
   You can also specify the “Any” list type.
6. Click **Continue**.
   The details of the uploaded file appear.
7. Click **Continue**.
   The final details of the uploaded list appear.
8. Confirm the details, and make sure the list type is set to **Domain** or **Any**.
9. Click **Save**.

   You can now select the list for the Uncategorized Sites option in an HTTP policy.

14 User Accounts

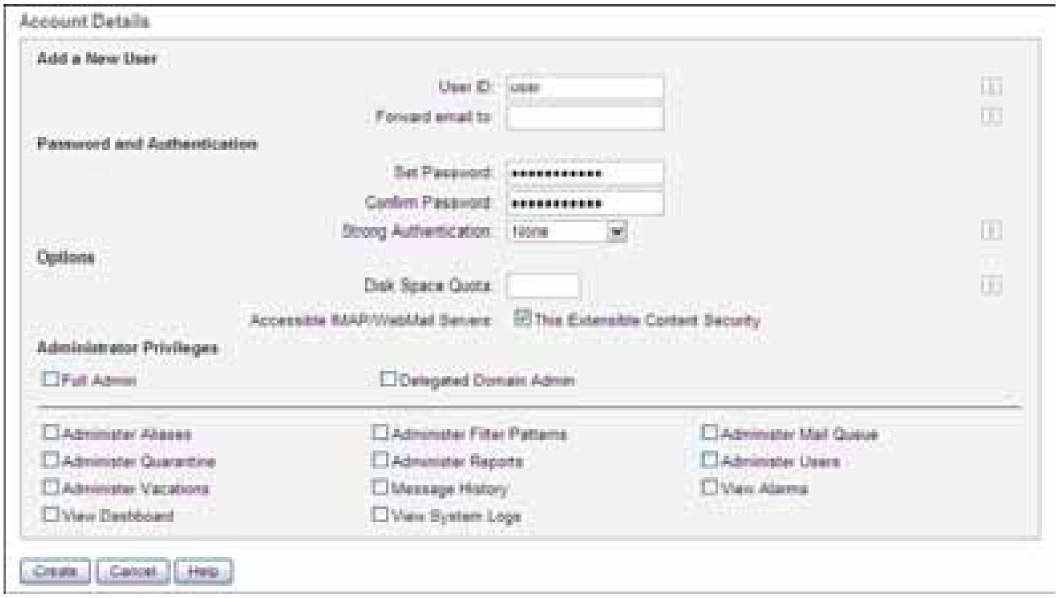
Local User Accounts

Local user accounts are available on the WatchGuard XCS that you can use for local mailboxes, admin accounts, web mail access, User Spam Quarantine, and Trusted/Blocked User Lists.

> ***Note*** *Local users are not available on cluster systems, except for admin users.*

To create a local account:

1. Select **Administration > Accounts > Local Accounts**.
2. Click **Add**.



Account Details

Add a New User

User ID: user

Forward email to:

Password and Authentication

Set Password: ••••••••••••

Confirm Password: ••••••••••••

Strong Authentication: None

Options

Disk Space Quota:

Accessible IMAP/WebMail Servers: ☑ This Extensible Content Security

Administrator Privileges

☐ Full Admin ☐ Delegated Domain Admin

☐ Administer Aliases ☐ Administer Filter Patterns ☐ Administer Mail Queue

☐ Administer Quarantine ☐ Administer Reports ☐ Administer Users

☐ Administer Vacations ☐ Message History ☐ View Alarms

☐ View Dashboard ☐ View System Logs

3. In the **User ID** text box, type a mail box name for the user.
4. In the **Forward email to** text box, type an optional address to which to forward all mail.

5. In the **Set Password** text box, type a password for the user.

   The user should change this password the first time they log in. If you enable Strong Password Enforcement (configured in the admin user), the user password must be at least 6 characters and contain alphabetic and non-alphabetic characters.

6. In the **Confirm Password** text box, type the user password again for confirmation.
7. From the **Strong Authentication** drop-down list, select a strong authentication method, if required.

   See *Strong Authentication* for more detailed information.

8. In the **Disk Space Quota** text box, type the maximum disk space, in megabytes (MB), that this user can use.

   To disable the quota, leave this text box blank, or type `0`.

9. In the **Accessible IMAP/WebMail Servers** section, select any additional servers that this user can access for IMAP and WebMail.
10. In the **Administer Privileges** section, you can select additional privileges for this user for the Tiered Administration or Dedicated Domain Admin features.

    See *Tiered Administration* for details on tiered admin privileges.

    See *Delegated Domain Administration* for details on Delegated Domain Administration.

Upload and Download User Lists

You can upload a list of local accounts in a text file. The file must contain comma or tab separated entries with one entry per line.

Use this format:

```
[login],[password],[email address],[quota in MB]
```

For example:

```
user1,ajg7rY,user1@example.com,0
user2,gh39ds,user2@example.com,100
```

You must use a text editor to create the file user.csv.

To update a local account list:

- To download the local account list from the WatchGuard XCS, click **Download File**.
- Open the file and update the local account list.
- Click **Upload File** and upload the edited file to the WatchGuard XCS.

> ***Note*** *When you upload a user list, it does not store any Tiered Admin settings. You must select Tiered Admin privileges in the user account page.*

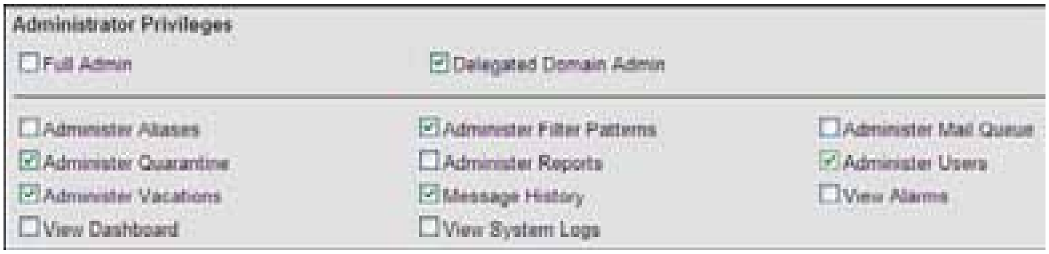
Tiered Administration

Tiered Administration allows you to assign additional administrative access permissions on a per-user basis. For example, to designate another user as an alternate administrator, you can select the **Full Admin** option in their user profile. To distribute administrative functions, you can configure more selective permissions to only authorize a user for certain tasks, for example, administer users and reports, configure Anti-Spam filter patterns, or view the Message History database.

> ***Note*** *You cannot assign LDAP users tiered admin privileges.*

To enable tiered admin privileges:

1. Select **Administration > Accounts > Local Accounts**.
2. Select a specific user profile.



Administrator Privileges

☐ Full Admin ☑ Delegated Domain Admin

☐ Administer Aliases ☑ Administer Filter Patterns ☐ Administer Mail Queue
☑ Administer Quarantine ☐ Administer Reports ☑ Administer Users
☑ Administer Vacations ☑ Message History ☐ View Alarms
☐ View Dashboard ☐ View System Logs

3. Select the corresponding check box to enable a specific admin privilege.

Full Admin

The user has administrative privileges equivalent to the admin user.

Administer Aliases

The user can add, edit, remove, upload, and download aliases (this excludes LDAP aliases.)

Administer Filter Patterns

The user can add, edit, remove, upload, and download Pattern Filters and Specific Access Patterns.

Administer Mail Queue

The user can administer mail queues.

Administer Quarantine

The user can view, delete, and send quarantined files.

Administer Reports

The user can view, configure and generate reports, and view system activity.

Administer Users

The user can add, edit, and relocate user mailboxes (except the Full Admin users). This includes the ability to upload and download user lists. The user can also configure User vacation notifications.

Administer Vacations

The user can edit local user's vacation notification settings and other global vacation parameters.

Message History

The user can view the Message History database and perform quick searches of the recent Mail and Web activity on the Dashboard.

View Dashboard

The user can view the Dashboard page. Tiered admins can only perform a quick search of the recent Mail and Web activity if Message History is also enabled.

View Alarms

The user can view the Alarms in the Alarms Indicator and the Local Alarms page, but cannot acknowledge them.

View System Logs

The user can view all system logs.

4. Click **Apply**.

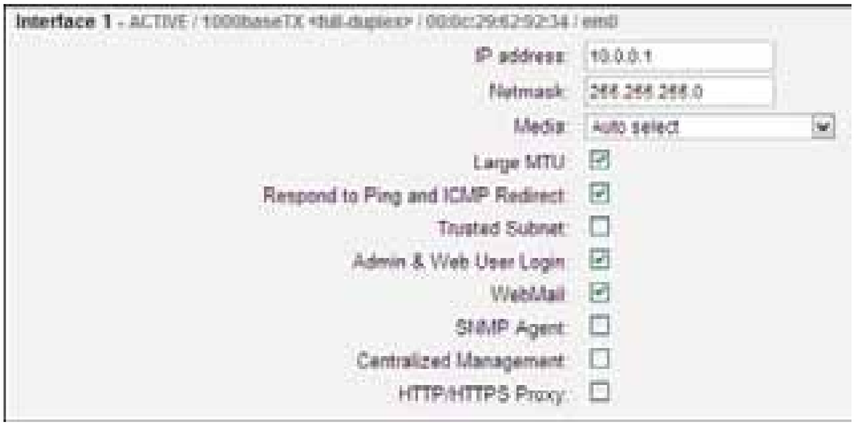
If you grant full or partial admin access to one or more user accounts, the actions performed by these administrators are logged because they have an identifiable UserID that is tracked by the WatchGuard XCS.

> **Note** *A user with Full Admin privileges cannot modify the profile of the Admin user, but they can edit other users with Full Admin privileges.*

Tiered Administration and WebMail Access

You must enable Tiered Admin and WebMail access on a network interface to allow Tiered Admin users to log in and administer the WatchGuard XCS.

1. Select **Configuration > Network > Interfaces**.
2. Select the **Admin & Web User Login** and **Webmail** check boxes on the required network interface.



Interface 1 - ACTIVE / 1000baseTX <full-duplex> / 00:0c:29:62:92:34 / em0

IP address: 10.0.0.1

Netmask: 255.255.255.0

Media: Auto select

Large MTU: ☑

Respond to Ping and ICMP Redirect: ☑

Trusted Subnet: □

Admin & Web User Login: ☑

WebMail: ☑

SNMP Agent: □

Centralized Management: □

HTTP/HTTPS Proxy: □

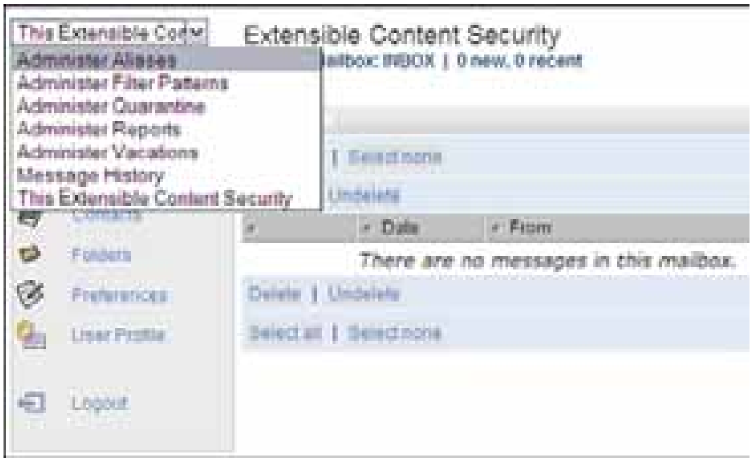
3. Click **Apply**.
   You must restart the system.

Log In with Tiered Administration Privileges

When you assign tiered admin privileges to a user, they can access the corresponding administrative functions through the WebMail client interface.

To log in as a Tiered Administrator:

1. Log in to the WatchGuard XCS device.
2. Select the feature to administer from the drop-down list.



Delegated Domain Administration

Delegated Domain Administration allows the primary administrator to delegate to specific users administrative rights to manage settings for a specific domain with domain policies.

The Delegated Domain Administrator can login to the WatchGuard XCS through the WebMail interface and configure and manage these settings for their specific domains:

- Manage settings for their domain with a subset of configuration options in a Domain Policy
  - Anti-Virus actions and Notifications
  - Anti-Spam controls: Certainly, Probably, and Maybe Spam Thresholds and Actions
  - Intercept Component Weights
  - Attachment Control Inbound and Outbound Attachment Types, Actions, and Notifications
  - Email Annotations
- Manage the Quarantine for their Delegated Domain
  - The Delegated Domain Administrator can view messages, delete messages, or release them from the quarantine to the end user.

The primary WatchGuard XCS administrator must create Delegated Domains and assign the Delegated Domain Admin for each domain. You can add Delegated Domains manually or upload them using a list of Delegated Domains and corresponding Delegated Domain Admins. You can delegate multiple domains to a single Delegated Domain Administrator, and you can assign multiple administrators to a Delegated Domain.

> ***Note*** *The Delegated Domain Administration configuration does not support Centralized Management.*

Delegated Domain Administration and Clustering

Delegated Domains on the Primary cluster device are replicated to other devices in the cluster. To manage the Delegated Domain policy, the Delegated Domain Administrator only needs to log in to the Primary device to manage the domain settings. The configuration is replicated to all other devices in the cluster.

In a cluster, you must configure Delegated Domain Policies on the Primary, and not the Secondary or other cluster devices. The configuration is automatically synchronized with the other devices in the cluster.

To view and manage the Quarantine for a domain, the Delegated Domain Administrator must log in to each device in the cluster as required, because each device stores its own dedicated quarantine area.

On a cluster, you can create Delegated Domain Administrators in the **Administration > Accounts > Tiered Admin** menu on the cluster Primary device.

Delegated Domain policies

The WatchGuard XCS automatically creates new domain policies and domain policy assignments for each new delegated domain you upload or manually create. Each policy uses the name of the delegated domain and you can view the policy in the **Policies** menu.

The Delegated Domain Administrator can log in to the WatchGuard XCS through WebMail and administer a subset of the policy for their domain.

Each delegated domain policy is automatically associated with the domain. To view these domain policy associations, select **Security > Policies > Domain Policy**.

To delete a delegated domain policy and its association, select **Administration > Accounts > Delegated Domains** and delete the delegated domain. The domain policies are automatically deleted when you delete the corresponding delegated domain.

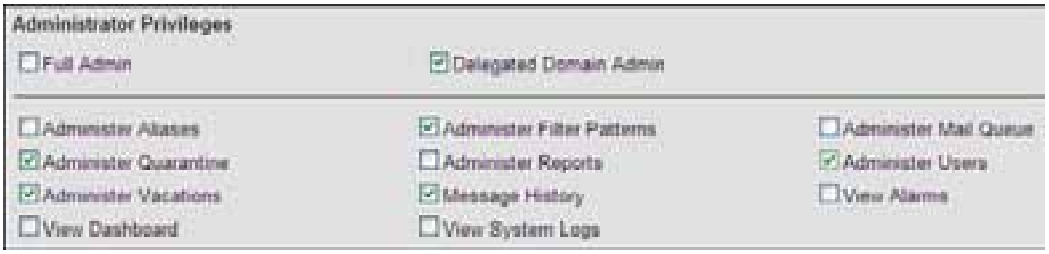
Create a Delegated Domain Administrator

To create a delegated domain administrator:

1. Select **Administration > Accounts > Local Accounts**.

   On a cluster Primary, select **Administration > Accounts > Tiered Admin**.
2. Create a new user, or modify an existing user.
3. In the **Administrator Privileges** section, select the **Delegated Domain Admin** check box.

> ***Note*** *The Full Admin and other Tiered Admin privileges are not available or supported when you select the Delegated Domain Admin option.*



Administrator Privileges

□ Full Admin ☑ Delegated Domain Admin

□ Administer Aliases ☑ Administer Filter Patterns □ Administer Mail Queue
☑ Administer Quarantine □ Administer Reports ☑ Administer Users
☑ Administer Vacations ☑ Message History □ View Alarms
□ View Dashboard □ View System Logs

4. If you have not yet created the corresponding Delegated Domain, you must create the domain in **Administration > Accounts > Delegated Domains**.
   You can also select the Delegated Domain Admin user for the domain on the Delegated Domains page.

   If you have already created Delegated Domains, a list of Delegated Domains appears. Select which domains this user can administer. You can assign more than one Delegated Domain to the user.
5. Click **Create** or **Apply** to save the user's settings.

Create Delegated Domains

You must create local users (or Tiered Admin users in a Cluster) before you create a Delegated Domain to assign an existing local user as the Delegated Admin for the domain. For a large number of delegated domains, we recommend that you upload a list of Delegated Domains and Admin users.

When you create a new delegated domain, the WatchGuard XCS automatically creates new domain policies, domain policy assignments, and the domain administrator users.

For example, for the delegated domain entry:

```
example.com, admin1@example.com
```

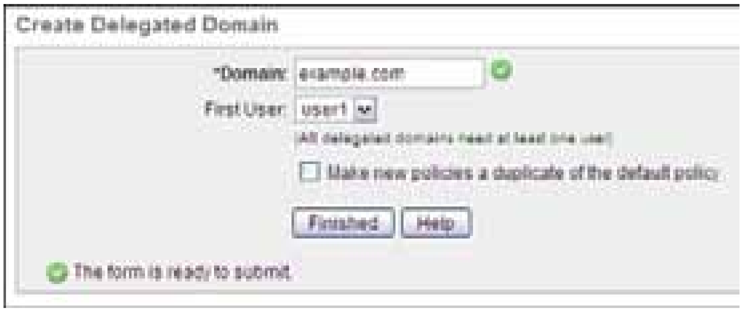
These items are created:

- A new delegated domain called example.com assigned to the administrator admin1@example.com.
- A new admin1 user with delegated domain permissions for the example.com domain.
- A new policy called example.com.
- A domain policy association between the domain example.com, and the delegated domain policy example.com.

To create a Delegated Domain and assign an administrator:

1. Select **Administration > Accounts > Delegated Domains**.
2. Select **Create Delegated Domain**.
3. In the **Domain** text box, type the domain name.

   For example, `example.com`.



Create Delegated Domain

*Domain: example.com

First User: user1

(All delegated domains need at least one user)

□ Make new policies a duplicate of the default polic

The form is ready to submit.

4. From the **User** drop-down list, select an administrator that is the first administrative user for this domain.
   To appear in this list, the user must already exist as a local user.

   > ***Note*** *You cannot assign Full admins and Tiered Admin the Delegated Domain Admin permission, and these users do not appear in the drop-down list of admins.*

   You can add more delegated domain administrators for the domain in **Administration > Accounts > Local Accounts** (or **Administration > Accounts >Tiered Admin** on a cluster Primary.)

5. New domain policies are automatically created for each new Delegated Domain.

   To make these new policies use the Default policy values, select the **Make new policies a duplicate of the default policy** check box.

   Clear this check box to assign the new domain policies as **Undefined**.

6. Click **Finished**.

Delete a Delegated Domain

To delete a delegated domain, click the **Delete** link beside a specific domain.

If you delete a delegated domain, this action also deletes the associated domain policies and domain policy assignments for that domain. Delegated domain admin users are not affected if you delete the domain they administer.

Upload Delegated Domains

You can upload a list of delegated domains and associated domain administrator email addresses. The list source can be an existing list (configured in **Security > Content Control > Dictionaries & Lists**), or you can upload a file from the Delegated Domains page.

> ***Note*** *Do not upload users who already exist as Full Admin or Tiered Admin users.*

To upload a list of delegated domains and administrators:

1. Select **Administration > Accounts > Delegated Domains**.
2. Click **Upload Delegated Domains**.
3. From the **Existing List** drop-down list, select a list, or click **Browse** to select a file to upload.

   Create this as a text file with this format:

   ```
   domain, admin-email
   ```

For example,

```
example.com, admin1@example.com
```

You can assign multiple domain administrators for each domain with multiple entries.

For example,

```
example.com, admin1@example.com
example.com, admin2@example.com
example.com, admin3@example.com
```

Specific administrators can be a domain administrator for multiple delegated domains.

For example,

```
example1.com, admin1@example.com
example2.com, admin1@example.com
example3.com, admin1@example.com
```

4. To make these new policies use the current Default policy values, select the **Make new policies a duplicate of the default policy** check box.
   Clear this check box to leave the domain policies as initially undefined.
5. Click **Continue**.
   The list is merged with any existing entries.

When you upload a new delegated domain and domain administrator, the WatchGuard XCS automatically creates new domain policies, domain policy assignments, and the domain administrator local user.

For example, for the delegated domain entry:

```
example.com, admin1@example.com
```

These items are created:

- A new delegated domain called example.com assigned to the administrator admin1@example.com.
- A new admin1 user with delegated domain permissions for the example.com domain.
- A new policy called example.com.
- A domain policy association between the domain example.com, and the delegated domain policy example.com.

Upload Delegated Domain Administration Users

If an administrative user for a delegated domain does not exist before the domain list upload, the WatchGuard XCS automatically creates the user. For example, for the administrative user admin1@example.com, the system creates this local username and password:

- Username: admin1.example.com
- Password: admin1

> **Note** *Users created automatically have the domain name appended to their username. When you create local accounts, they do not append the domain name.*

This user is managed in **Administration > Accounts > Local Accounts**, (or **Administration > Accounts > Tiered Admin** on a cluster Primary). The **Delegated Domain Admin** option and their corresponding domains are automatically selected for the user.

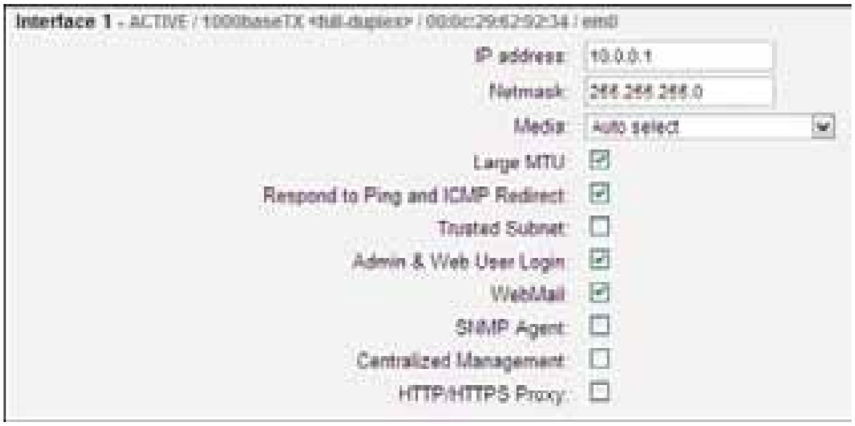
Administer Delegated Domains

To administer a domain, the delegated domain administrator must log in to the WatchGuard XCS through WebMail where they can access a subset of configuration options to customize for their domain.

You must enable the **WebMail** and **Admin & Web User Login** options on a network interface to allow delegated domain admins to log in to the WatchGuard XCS.

To enable **WebMail** and **Admin & Web User Login** on a network interface:

1. Select **Configuration > Network > Interfaces**.



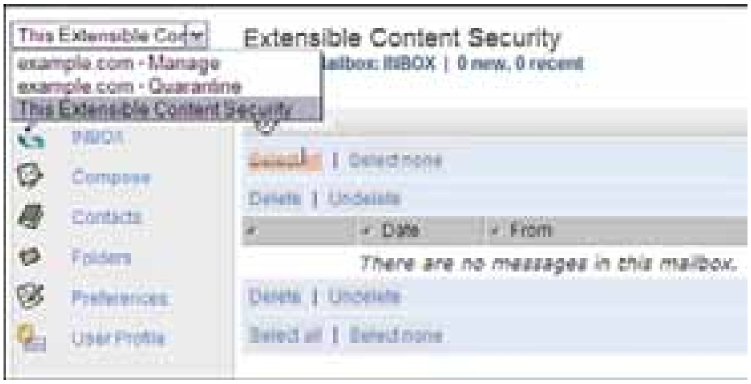
Interface 1 - ACTIVE / 1000baseTX <full-duplex> / 00:0c:29:62:92:34 / em0

IP address: 10.0.0.1
Netmask: 255.255.255.0
Media: Auto select
Large MTU: ☑
Respond to Ping and ICMP Redirect: ☑
Trusted Subnet: □
Admin & Web User Login: ☑
WebMail: ☑
SNMP Agent: □
Centralized Management: □
HTTP/HTTPS Proxy: □

2. Select the **WebMail** and **Admin & Web User Login** check boxes on the required interface.
3. Click **Apply**.
   You must restart the system.

Log in to Delegated Domain Administration

To login to a delegated domain to administer its policies, the delegated domain administrator must log in directly to the WatchGuard XCS with their login name, for example, admin1 (or admin1.example.com if the user was created in an uploaded list).



Select a domain and function from the drop-down list in the top-left corner of the page. If the delegated domain administrator is associated with multiple domains, the drop-down list contains links to all the domains to which they are assigned.

- To manage the delegated domain policy, select the **Manage** link.
- To view the messages in the delegated domain quarantine area, click the **Quarantine** link.

Manage the Delegated Domain

1. To modify the configuration for the Domain policy, select the **Manage** option for the Delegated Domain.
   This policy only provides a subset of the full policy configuration for the Delegated Domain Admin user to manage. The primary WatchGuard XCS Administrator still has full access to all options in the Domain Policy.

   > ***Note*** *In a cluster, you must always configure the Delegated Domain Policies on the Primary cluster device. The configuration is automatically synchronized with the other devices in the cluster.*

   These policy items are available to configure:

   - Anti-Spam and Anti-Virus
     - Anti-Virus Actions and Notifications
     - Anti-Spam Controls – Certainly, Probably, and Maybe Spam Thresholds and Actions
     - Intercept Component Weights
   - Attachment Control – Inbound and Outbound Attachment Types, Actions, and Notifications
   - Email – Annotations
2. Click **Apply** to save the settings for this policy.

View the Delegated Domain Quarantine

Any message security features that quarantine mail, for example, Anti-Virus, Anti-Spam, and Attachment Control, place the mail messages in the quarantine area. To view the Quarantined messages for this specific delegated domain, select the **Quarantine** option.

Click on a *Queue ID* to view the details of a message, or click **Delete** to delete the message from the quarantine. Quarantined messages can also be released from the quarantine and delivered to their original destination by clicking the **Release** button.

The delegated domain administrator can view messages, delete messages, or release them from the quarantine to the end user. In a cluster environment, the delegated domain administrator must log in to each device in the cluster to view and manage its quarantine area.

Use the search field to look for specific messages within the quarantine. For example, you can search for the name of a specific virus so that any quarantined messages infected with that specific virus appear.

Use the **Delete All** and **Release All** buttons specifically with the search function. You must enter a specific search pattern before you use these controls.

Mirror Accounts

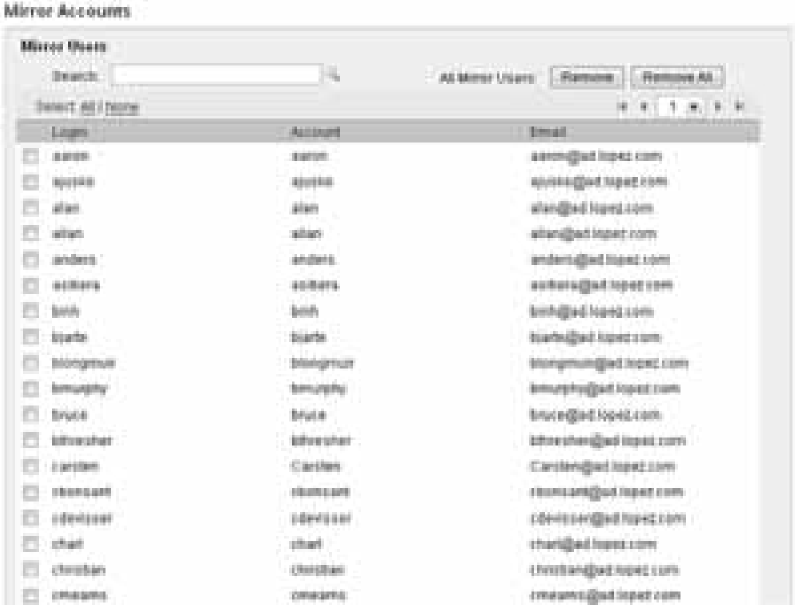
You can import LDAP user accounts from a directory server and mirror them locally. This allows you to create local accounts to allow these users to log in locally for the Spam Quarantine and Trusted/Blocked Senders features.

These mirror accounts are not local accounts that can accept mail. Local accounts are only used for the Spam Quarantine and Trusted/Blocked Senders features.

See *Directory Users* for more detailed information on creating mirror accounts.

To display all mirrored users:

1. Select **Administration > Accounts > Mirror Accounts**.
   The Mirror Accounts page appears.



Login	Account	Email
□ aaron	aaron	aaron@ad.lopez.com
□ ajuska	ajuska	ajuska@ad.lopez.com
□ alan	alan	alan@ad.lopez.com
□ allan	allan	allan@ad.lopez.com
□ anders	anders	anders@ad.lopez.com
□ aolbers	aolbers	aolbers@ad.lopez.com
□ binh	binh	binh@ad.lopez.com
□ bjarte	bjarte	bjarte@ad.lopez.com
□ blongmuir	blongmuir	blongmuir@ad.lopez.com
□ bmurphy	bmurphy	bmurphy@ad.lopez.com
□ bruce	bruce	bruce@ad.lopez.com
□ bthresher	bthresher	bthresher@ad.lopez.com
□ carsten	Carsten	Carsten@ad.lopez.com
□ cbonsaint	cbonsaint	cbonsaint@ad.lopez.com
□ cdevisser	cdevisser	cdevisser@ad.lopez.com
□ chad	chad	chad@ad.lopez.com
□ christian	christian	christian@ad.lopez.com
□ cmearns	cmearns	cmearns@ad.lopez.com

2. To remove selected individual user mirror accounts, click **Remove**.

   To show only the local users on this WatchGuard XCS, click **Show Local Users**.

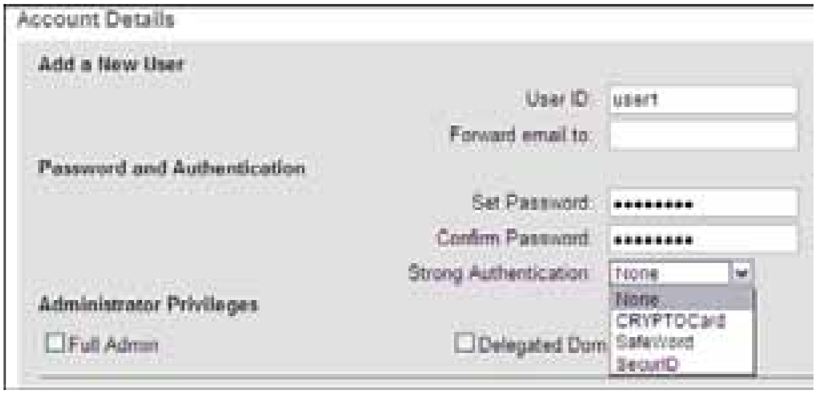
   Use the **Remove All** button with the search function. You must enter a specific search pattern before you click **Remove All** to delete the results.

Strong Authentication

By default, user authentication is based on User ID and password. The WatchGuard XCS also supports strong authentication methods, for example, CRYPTOCard, SafeWord, and RSA SecurID. These hardware token devices provide an additional authentication key that you must provide in addition to the User ID and password.

To configure strong authentication:

1. Select **Administration > Accounts > Local Accounts**.
2. Select a **Strong Authentication** method.



Account Details

Add a New User

User ID: user1

Forward email to:

Password and Authentication

Set Password: ●●●●●●●●●

Confirm Password: ●●●●●●●●●

Strong Authentication: None

Administrator Privileges

□ Full Admin

□ Delegated Dom

3. Click **Apply**.

CRYPTOCard

The CRYPTOCard option is supported by a local authentication server and requires no external system for authentication. When you select CRYPTOCard, you are prompted to program the card with the token configuration wizard. The WatchGuard XCS only supports manually programmable CRYPTOCard RB-1 tokens.

SafeWord

SafeWord Platinum and Gold tokens are supported by a local authentication server, and require no external system for authentication. When you select SafeWord, you are prompted to program the card with the token configuration wizard. The WatchGuard XCS only supports manually programmable SafeWord tokens.

SecurID

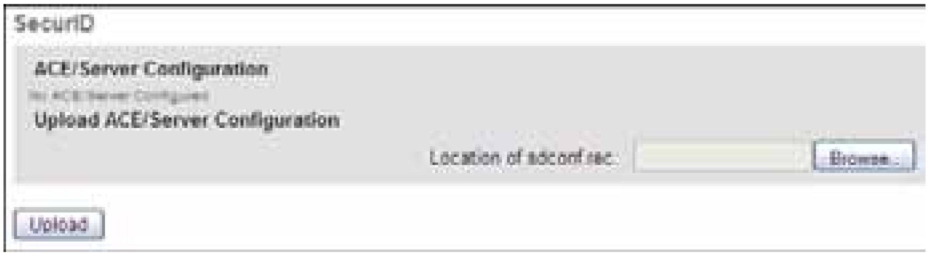
To configure RSA SecurID, you must set up the WatchGuard XCS as a valid client on the ACE Server, and create an sdconf.rec (ACE Agent version 4.x) file and upload it to the XCS device. The WatchGuard XCS supports newer ACE server versions, but the sdconf.rec file must be in ACE Agent version 4.x format.

SecurID

To configure RSA SecurID, you must set up the WatchGuard XCS as a valid client on the ACE Server, and create an sdconf.rec (ACE Agent version 4.x) file and upload it to the XCS device. The WatchGuard XCS supports newer ACE server versions, but the sdconf.rec file must be in ACE Agent version 4.x format.

> ***Note*** *Make sure that the WatchGuard XCS domain name is listed in your DNS server. SecurID authentication does not work properly if a DNS record does not exist.*

1. Select **Administration > Accounts > SecurID**.
   The SecurID page appears.



SecurID

ACE/Server Configuration

No ACE/Server Configured

Upload ACE/Server Configuration

Location of sdconf.rec:

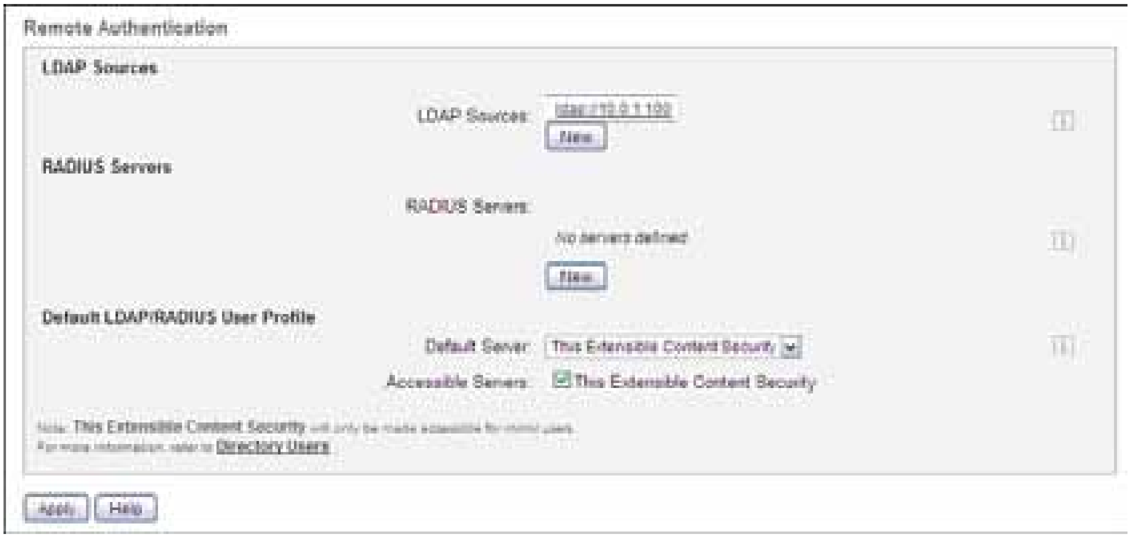
2. Click **Browse** to locate a sdconf.rec file on your local workstation.
3. Click **Upload**.
4. Select **Configuration > Network > Interfaces** and enable **SecurID** on a network interface.
5. Click **Apply**.
   You must restart the device.

Remote Accounts and Directory Authentication

Directory authentication allows users to authenticate to the WatchGuard XCS without a local account. When an unknown user logs in, the WatchGuard XCS sends the User ID and password to the specified LDAP or RADIUS server. If the user successfully authenticates, the WatchGuard XCS logs them in and provides access to the specified servers.

LDAP and RADIUS provide a convenient way to allow access to internal mail servers or webmail servers, for example, Outlook Web Access (OWA). Users that log in locally to an Exchange server based on an Active Directory identity can use the same identity to use Outlook Web Access with the Secure WebMail service.

If you define both LDAP and RADIUS authentication services, the WatchGuard XCS tries to authenticate with RADIUS first, and then LDAP if RADIUS authentication fails.



Remote Authentication

LDAP Sources

LDAP Sources: ldap://10.0.1.100

RADIUS Servers

RADIUS Servers:

No servers defined

Default LDAP/RADIUS User Profile

Default Server: This Extensible Content Security

Accessible Servers: ☑ This Extensible Content Security

Note: This Extensible Content Security will only be made accessible for mirror users.
For more information, refer to Directory Users

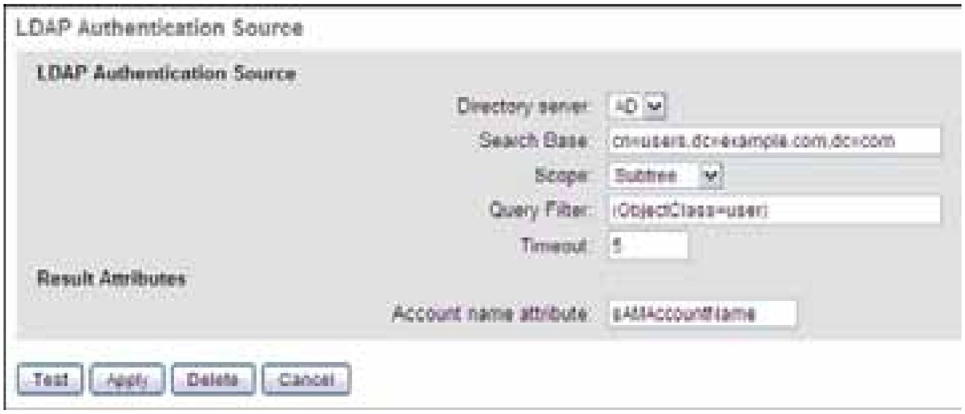
The server “This WatchGuard XCS” is only accessible to mirror users imported from an LDAP directory. See *Directory Users* for more detailed information on mirrored accounts.

The other servers listed in the **Accessible Servers** section are configured in **Configuration > WebMail > WebMail**. See *Secure WebMail* for more detailed information on configuring this feature.

Configure LDAP Authentication

To configure LDAP for authentication:

1. Select **Administration > Accounts > Remote Authentication**.
2. Click the **New** button in the **LDAP Sources** section to define a new LDAP source.



LDAP Authentication Source

LDAP Authentication Source

Directory server: AD

Search Base: cn=users,dc=example.com,dc=com

Scope: Subtree

Query Filter: (ObjectClass=user)

Timeout: 5

Result Attributes

Account name attribute: sAMAccountName

3. In the **Directory Server** drop-down list, select a configured LDAP directory server for authentication.
4. In the **Search Base** text box, type the starting base point to start the search from.

   For example, `cn=users,dc=example,dc=com`.

5. From the **Scope** drop-down list, select the scope of the search.

   - **Base** – Searches the base object only.
   - **One Level** – Searches objects one level beneath the base object, but excludes the base object.
   - **Subtree** – Searches the entire subtree of which the base distinguished name is the topmost object. This includes the base object.

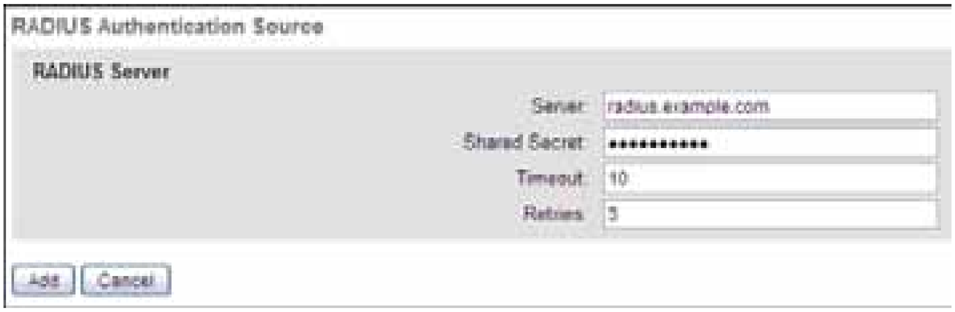
4. In the **Query Filter** text box, type a specific query filter to search for a user in your LDAP directory hierarchy.

   For Active Directory, type `(ObjectClass=user)`.

5. In the **Timeout** text box, type the maximum interval, in seconds, to wait for the search to complete.
   The default is 5. You must enter a between 1 and 100.
6. In the **Account name attribute** text box, type the account name result attribute that identifies a user's login or account name. For Active Directory, type `sAMAccountName`.
7. Click **Apply**.

RADIUS Authentication

1. Select **Administration > Accounts > Remote Authentication**.
2. Click **New** in the **RADIUS Server** section.
   The RADIUS Authentication Source page appears.



RADIUS Authentication Source

RADIUS Server

Server: radius.example.com

Shared Secret: ••••••••••••

Timeout: 10

Retries: 3

3. In the **Server** text box, type the FQDN or IP address of the RADIUS server.
4. In the **Shared Secret** text box, type the password for the RADIUS server.

   A shared secret is a text string that acts as a password between a RADIUS server and client. Choose a secure shared secret of at least 8 characters in length, and include a mixture of upper and lowercase alphabetic characters, numbers, and special characters, for example, the "@" symbol.

   When you add a RADIUS server, the administrator of the RADIUS server must also list this WatchGuard XCS as a client with the same shared secret. All listed RADIUS servers must contain the same users and credentials.

5. In the **Timeout** text box, type a maximum timeout value, in seconds, to contact the RADIUS server.
   The default is 10 seconds.
6. In the **Retry** text box, type a time interval, in seconds, to retry a connection attempt to the RADIUS server.
   The default is 3 seconds.
7. Click **Add**.

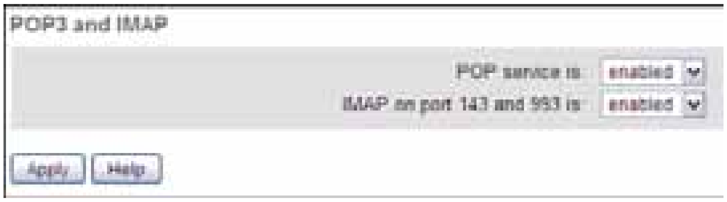
POP3 and IMAP Access

Mail is delivered to local mailboxes after the same processing that applies to all other destinations. Users can use any POP3 or IMAP-based mail client to download their messages from a local mailbox. User's can also access their mailboxes through the WatchGuard XCS WebMail client.

> ***Note*** *Use the secure versions of POP and IMAP to make sure passwords are not transmitted in clear text.*

To configure POP3 and IMAP Access:

1. Select **Configuration > Mail > POP3 and IMAP**.
   The POP3 and IMAP page appears.

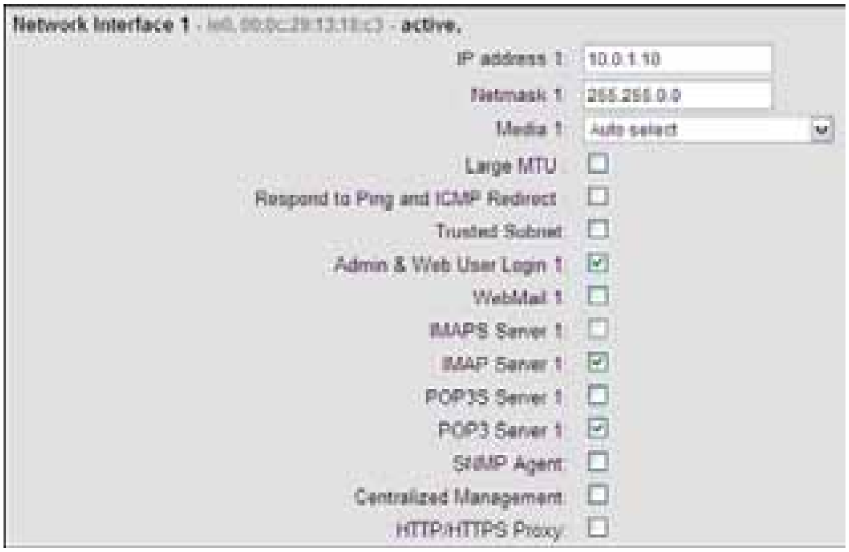


POP3 and IMAP

POP service is: enabled

IMAP on port 143 and 993 is: enabled

2. From the **POP service is** drop-down list, select **enabled** to enable POP and secure POP access.
3. From the **IMAP on port 143 and 993 is** drop-down list, select **enabled** to enable IMAP and secure IMAP access.
4. Select **Configuration > Network > Interfaces**.



Network Interface 1 - le0, 00:0c:29:13:18:c3 - active.

IP address 1:	10.0.1.10
Netmask 1:	255.255.0.0
Media 1:	Auto select
Large MTU	□
Respond to Ping and ICMP Redirect	□
Trusted Subnet	□
Admin & Web User Login 1	☑
WebMail 1	□
IMAPS Server 1	□
IMAP Server 1	☑
POP3S Server 1	□
POP3 Server 1	☑
SNMP Agent	□
Centralized Management	□
HTTP/HTTPS Proxy	□

5. On the required network interface:

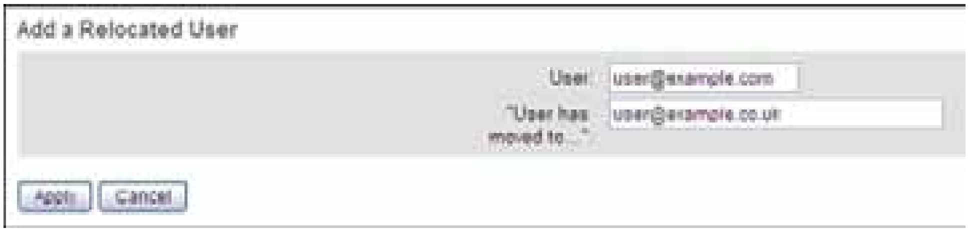
   - Select the **IMAPS Server** check box to enable access to secure IMAP on this interface.
   - Select the **IMAP Server** check box to enable access to IMAP on this interface.
   - Select the **POP3S Server** check box to enable access to secure POP on this interface.
   - Select the **POP Server** check box to enable access to POP on this interface.

6. Click **Apply**.
   You must restart the device.

Relocated Users

Use the *Relocated Users* page to return information to the sender of a message on how to reach users that no longer have an account on the WatchGuard XCS. You can also specify a full domain if the address has changed for a large number of users.

1. Select **Administration > Accounts > Relocated Users**.
2. Click the **Add** button to add a new relocated user.



Add a Relocated User

User:	user@example.com
"User has moved to..."	user@example.co.uk

3. In the User text box, type a user or domain name.

   For example, `user1`, `user1@example.com`, or `@example.com`.

4. In the **User has moved to...** text box, type the appropriate contact information for the relocated user, for example, their new email address, street address, or phone number.
5. Click **Apply**.

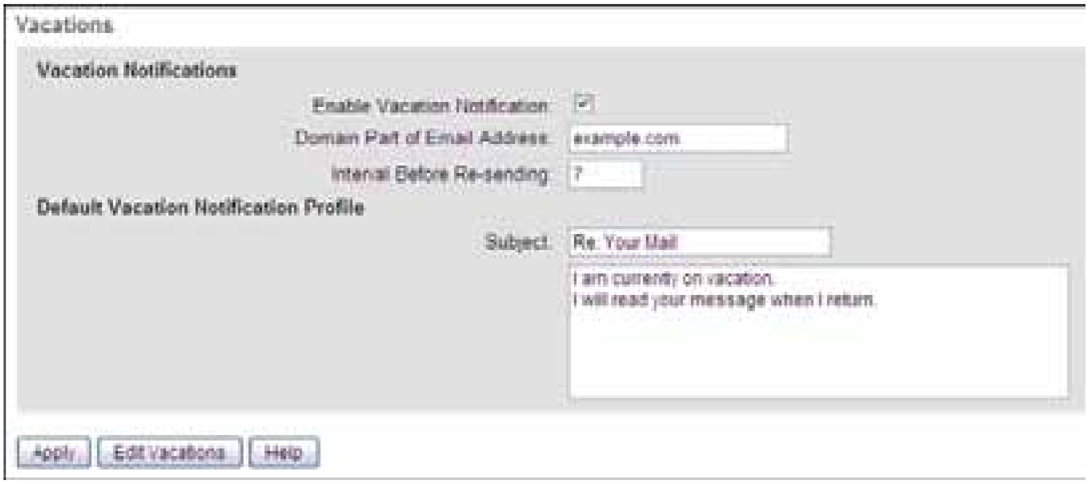
Vacation Notification

When a user is out of the office, they can enable the *Vacation Notification* feature that sends an automated email reply to incoming messages. The reply message is fully configurable, and allows a user to personalize their vacation notification message.

Vacation notifications are processed after mail aliases and mappings. You must create notifications for a specific end user and not for an alias or mapping. Vacation Notifications are not available in a cluster.

To enable Vacation Notifications:

1. Enable Vacation Notifications globally.
2. Configure individual settings:
3. Configure Vacation Notification for the user in the user configuration page.
4. The user configures their own Vacation Notification through WebMail.
5. To enable Vacation Notifications:
6. Select **Administration >Accounts > Vacations**.
   The Vacations page appears.



Vacations

Vacation Notifications

Enable Vacation Notification: ☑

Domain Part of Email Address: example.com

Interval Before Re-sending: 7

Default Vacation Notification Profile

Subject: Re: Your Mail

I am currently on vacation.
I will read your message when I return.

7. To enable Vacation Notifications globally for all users, select **Enable Vacation Notification**.
8. In the **Domain Part of Email Address** text box, type the domain name that is appended to local user names.

   For example, `example.com`.
9. In the **Interval Before Re-sending** text box, type the number of days to send a notification after a previous notification was sent, if a new email arrives from the original sender.
   The default is 7 days.
10. In the **Subject** text box, type the subject for the default notification message.
    Users can change the subject and message from their own user profile.
11. In the message text box, type the text for the Vacation Notification message.
    Users can change the message from their own user profile.

12. To see all Vacation Notification settings and to add arbitrary notifications for non-local users, click **Edit Vacations**.

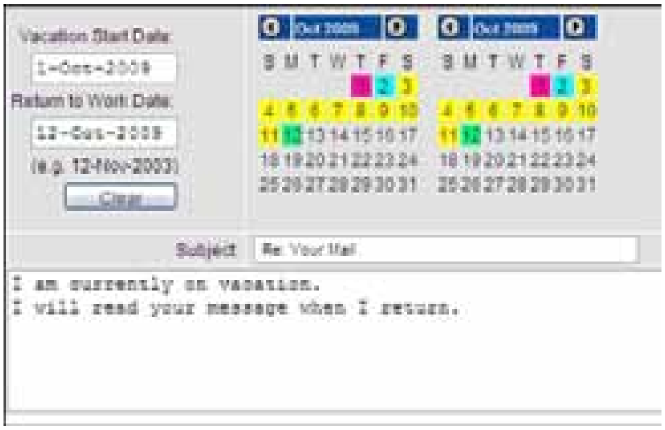
    Click on an existing email address to edit the user’s vacation notification settings, or type an address if this user has no vacations defined.
    From this page, you can configure the notification settings and the address from which incoming mail receives a vacation response.

User Vacation Notification Profile

You can configure vacation notifications for individual users in their user profile in the Local Accounts page. Users can configure their own Vacation Notification settings in their profile through the WebMail client.

To configure Vacation Notification:

1. Log in to the WebMail client.
2. Select **User Profile**.
3. Set the **Vacation Start Date** on the left calendar.
4. Set the **Return to Work Date** on the right calendar.
   The vacation notices are sent out automatically during this time.
5. Modify the default **Subject** and contents of the response message as required.



Vacation Start Date: 1-Oct-2009

Return to Work Date: 12-Oct-2009

(e.g. 12-Nov-2003)

Subject: Re: Your Mail

```
I am currently on vacation.
I will read your message when I return.
```

6. Click **Save User Profile**.

> **Note** *Vacation Notifications are not sent to bulk messages, for example, mailing lists and system generated messages. Vacation Notifications are also not sent to messages identified as spam.*

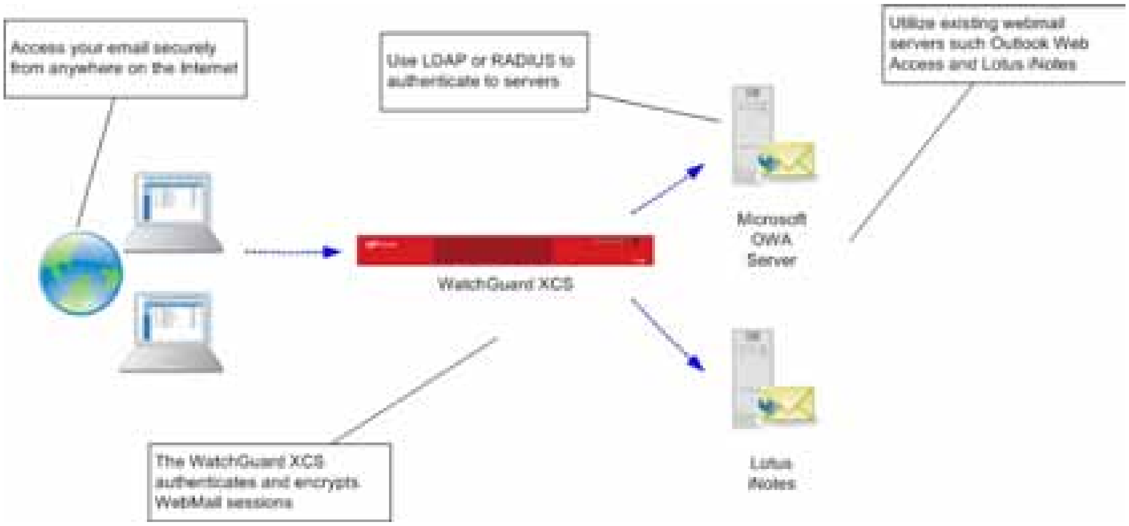
15 Secure WebMail

Secure WebMail

The *Secure WebMail* feature provides a highly secure mechanism to access webmail services, for example, Microsoft OWA (Outlook Web Access), Lotus iNotes, and IMAP servers. Webmail services provide a simple remote interface for users to access their mail server mailboxes remotely through a web browser.

Because these webmail services are accessible from the Internet, they present a number of security challenges. The Secure WebMail feature is designed to support the use of webmail services and protect Webmail servers from Internet attacks. The connection is managed using a full application proxy.

The WatchGuard XCS completely recreates all HTTP/HTTPS requests made by the external client to the internal webmail server.

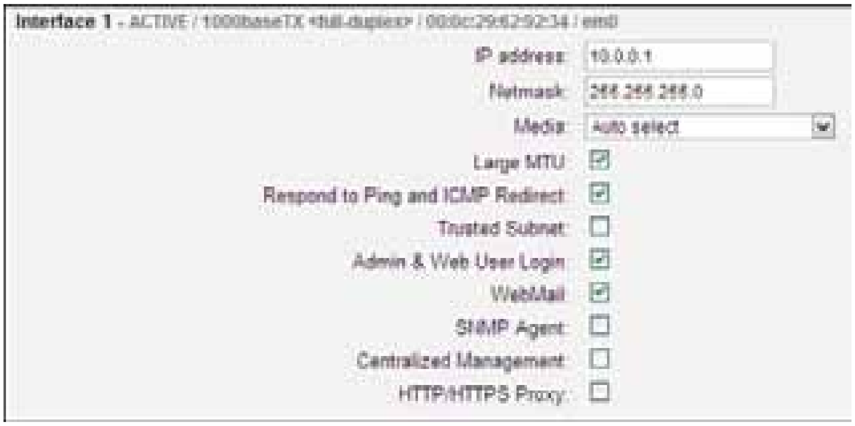

Access your email securely from anywhere on the Internet
Use LDAP or RADIUS to authenticate to servers
Utilize existing webmail servers such Outlook Web Access and Lotus iNotes
Microsoft OWA Server
WatchGuard XCS
The WatchGuard XCS authenticates and encrypts WebMail sessions
Lotus iNotes

> **Note** *In a clustered environment, you can only enable the Secure WebMail proxy on the Primary device in the cluster.*

Configure Secure WebMail

To enable and configure Secure WebMail servers:

1. Select **Configuration > Network > Interfaces**.
2. Select the **WebMail** check box on the required network interface.



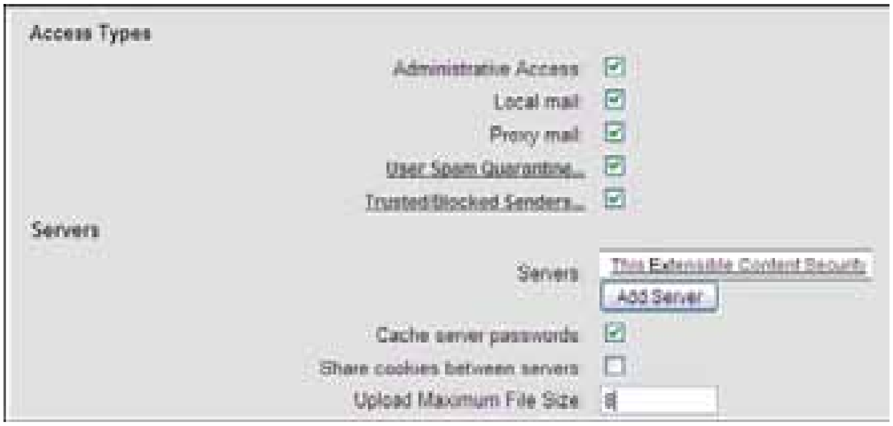
Interface 1 - ACTIVE / 1000baseTX <full-duplex> / 00:0c:29:62:92:34 / em0

IP address: 10.0.0.1
Netmask: 255.255.255.0
Media: Auto select
Large MTU: ☑
Respond to Ping and ICMP Redirect: ☑
Trusted Subnet: □
Admin & Web User Login: ☑
WebMail: ☑
SNMP Agent: □
Centralized Management: □
HTTP/HTTPS Proxy: □

3. Click **Apply**.

   You must restart the device.

4. Select **Configuration > WebMail > WebMail**.



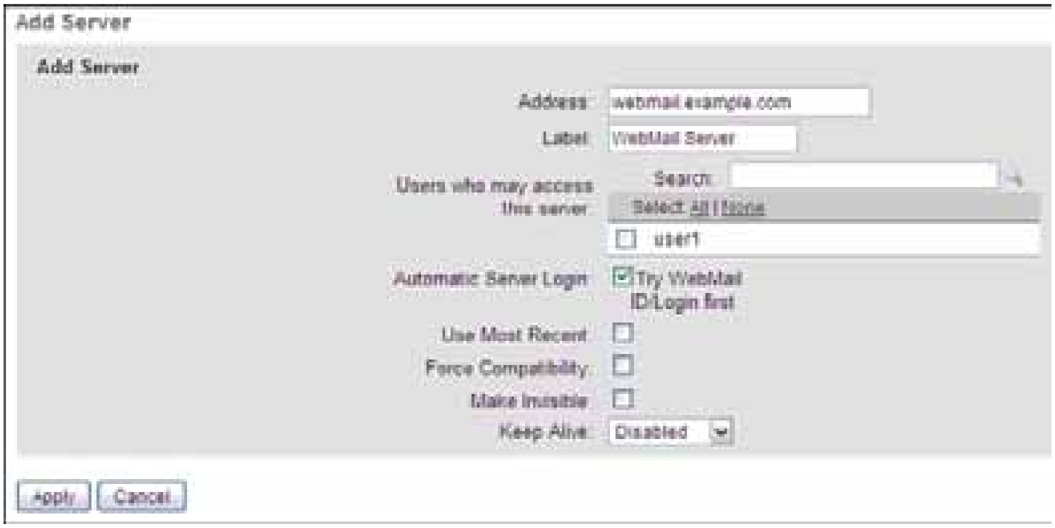
Access Types

Administrative Access ☑
Local mail ☑
Proxy mail ☑
User Spam Quarantine... ☑
Trusted/Blocked Senders... ☑

Servers

Servers: This Extensible Content Security
Add Server
Cache server passwords ☑
Share cookies between servers □
Upload Maximum File Size 8

5. In the **Servers** section, click **Add Server**.



Add Server

Add Server

Address: webmail.example.com

Label: WebMail Server

Users who may access this server: Search:

Select All | None

□ user1

Automatic Server Login: ☑ Try WebMail ID/Login first

Use Most Recent: □

Force Compatibility: □

Make Invisible: □

Keep Alive: Disabled

6. In the **Address** text box, type the IP address, hostname, or URL of the WebMail server.
   WebMail servers must be one of these servers: IMAP, Outlook Web Access (OWA), or Lotus iNotes.
7. In the **Label** text box, type an optional label to describe this server.
8. In the **Users who may access this server** section, select any local users who are able to access this server.
   If you use Remote Authentication and do not use local users, no additional configuration is required.

   To try the user's WebMail ID/Login first before prompting for an ID and password, select the **Automatic Server Login** check box.
   Leave this option disabled to force a login prompt for each new server. This option enables single login capabilities to allow users to login to the WatchGuard XCS and their WebMail server with only one login. Disable **Automatic Server Login** if the server is set to expire passwords after three failed attempts.

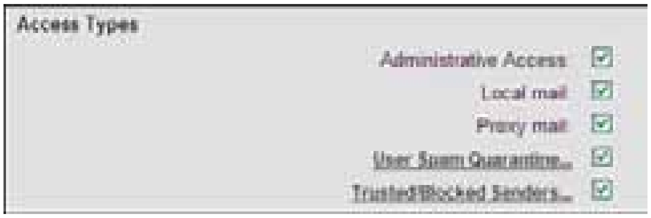
9. To try the most recent credentials first when the user switches servers, select the **Use Most Recent** check box.
   The Use Most Recent option only applies to users with more than one accessible WebMail server.
10. To allow support for Outlook Web Access 2000 and limited support for OWA 2003, select the **Force Compatibility** check box.
11. To make the server invisible to users in the Secure WebMail server drop-down list, select the **Make Invisible** check box.
12. From the **Keep Alive** drop-down list, select the frequency to send keep-alive messages to the WebMail server to keep the client connection alive.
13. You can set these additional options:

    - **Cached server passwords** – Enable this option to keep a copy of the user's password until they explicitly log out. If a user switches servers, they do not need to re-enter their password.
    - **Share cookies between servers** – Enable this option to make sure that when a user moves from server to server or is redirected to another server, the user's session cookies are also passed along.
    - **Upload Maximum File Size** – Type the maximum upload file size (in MB) allowed.

14. Click **Apply**.

Access Types

These options enable controls in the WebMail interface for features, for example, the Spam Quarantine, Trusted and Blocked Senders, and Administrative Access.



Access Types

Administrative Access ☑

Local mail ☑

Proxy mail ☑

User Spam Quarantine... ☑

Trusted/Blocked Senders... ☑

- **Administrative Access** – Enables access to administrative functions if the user has administrative privileges, for example, through Tiered Administration.
- **Local Mail** – Enables access to IMAP servers on the local network.
- **Proxy Mail** – Enable proxy mail access to other WebMail/IMAP servers. This is required for access to other web mail servers, for example, OWA for iNotes.
- **User Spam Quarantine** – Enables the Spam Quarantine controls.
- **Trusted/Blocked Senders List** – Enables the Trusted and Blocked Senders List controls.

For organizations that only want to use local mailboxes for the Spam Quarantine controls or Trusted Senders, we recommend that you disable **Local Mail** and **Proxy Mail** access, and enable **Personal Quarantine Controls** and **Trusted/Blocked Senders**. This displays only those functions to the end user when they log into the WebMail account. You can disable **Personal Quarantine** and **Trusted/Blocked Senders** if you only use the Spam Quarantine summary email for these features and do not require the users to log in locally.

> ***Note*** *You must enable at least one of these options o allow WebMail access on a specified interface in* ***Configuration > Network > Interfaces****. If you disable all of these access options, the WebMail access option on an interface is disabled.*

Configure Outlook Web Access

The Secure WebMail proxy provides a highly secure mechanism to access Microsoft OWA (Outlook Web Access). OWA uses a very similar interface to Outlook and provides an easy to use remote interface for users to access their Exchange mailboxes remotely. With OWA, users can see all of their mail, contacts, and calendar using a web browser.

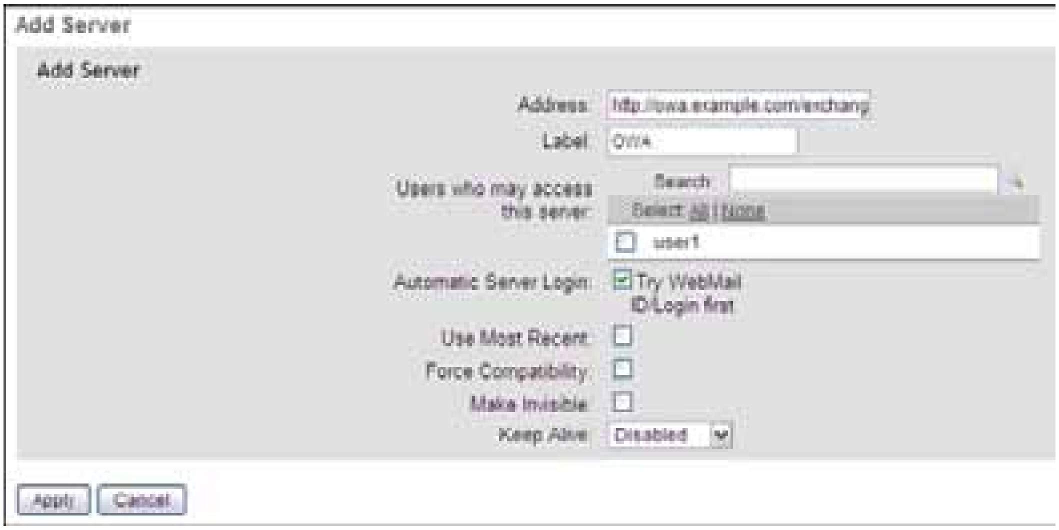
Because OWA is accessible from the Internet, its presents a number of security challenges. The Secure WebMail Proxy feature is designed to support OWA use and protect it from Internet attacks. The OWA connection is managed using a full application proxy. The WatchGuard XCS completely recreates all HTTP/HTTPS requests made by the external client to the internal OWA Exchange server. In a typical deployment, OWA users connect to the OWA interface on the public interface of the WatchGuard XCS. The WatchGuard XCS then proxies the traffic with its private interface to the OWA server. The connection is secure because the WatchGuard XCS recreates requests by the OWA clients.

If you deploy the WatchGuard XCS on the DMZ of a network firewall, OWA users first connect to the public interface of the network firewall. The traffic is forwarded to the WatchGuard XCS and then the requests are recreated and forwarded to the OWA server. On the network firewall, incoming port 443 needs to be opened from the public interface to the DMZ to allow traffic from the Internet to the WatchGuard XCS. You also open up port 80 from the DMZ to the private network to allow the WatchGuard XCS to connect to the OWA server.

Enable the Secure WebMail OWA Proxy

To configure the OWA proxy.

1. Select **Configuration > WebMail > WebMail**.
2. Click the **Add Server** button.



Add Server

Add Server

Address: http://owa.example.com/exchang

Label: OWA

Users who may access this server: Search:

Select All | None

□ user1

Automatic Server Login: ☑ Try WebMail ID/Login first

Use Most Recent: □

Force Compatibility: □

Make Invisible: □

Keep Alive: Disabled

3. In the **Address** text box, type the URL where OWA is located.

   For example,

   `http://owa.example.com/exchange/`

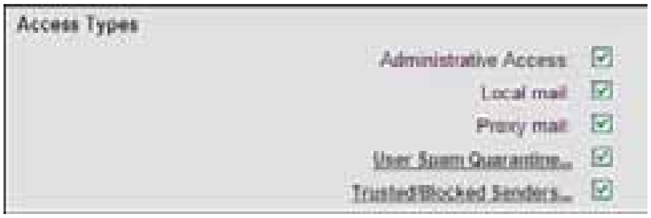
4. In the **Label** text box, enter an optional name to describe this server.
5. In the **Users who may access this server** section, select any local users that are allowed to use OWA.
   You can also enable this option from the user's individual mailbox properties. Users can also authenticate to OWA through Active Directory/LDAP.
6. The WatchGuard XCS sends the user account portion of the user's mail attribute (for example, user, in the address user@example.com) to the OWA server by default.

   If the LDAP user's *sAMAccountName* is equivalent to the *mail* attribute, select the **Try Webmail ID/login first** option.

   If this is different from the *sAMAccountName* attribute, clear the **Try Webmail ID/login first** check box. If this option is enabled, the user receives an invalid ID error message. The user then needs to enter their user name and password again to gain access to OWA.

7. Click **Apply**.
8. Select **Configuration > WebMail > WebMail**.

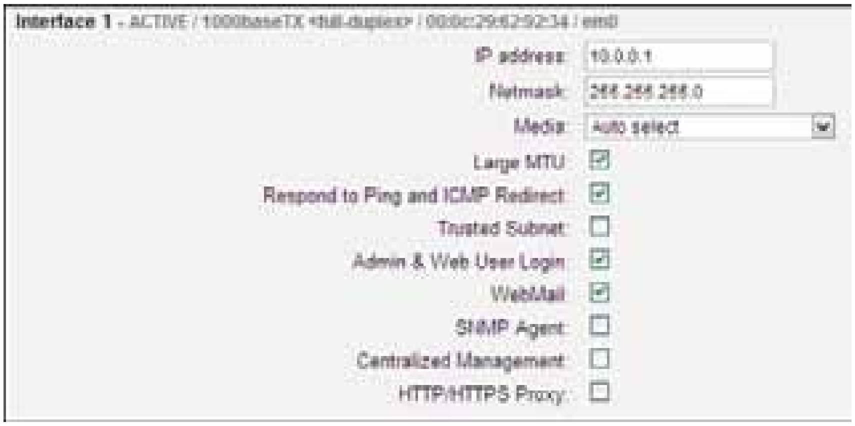
9. In the **Access Types** section, select the **Proxy mail** check box.



Access Types

Administrative Access ☑
Local mail ☑
Proxy mail ☑
User Spam Quarantine... ☑
Trusted/Blocked Senders... ☑

10. Click **Apply**.
11. Select **Configuration > Network > Interfaces**.
12. Select the **WebMail** check box on the network interface from which users are accessing WebMail.



Interface 1 - ACTIVE / 1000baseTX <full-duplex> / 00:0c:29:62:92:34 / em0

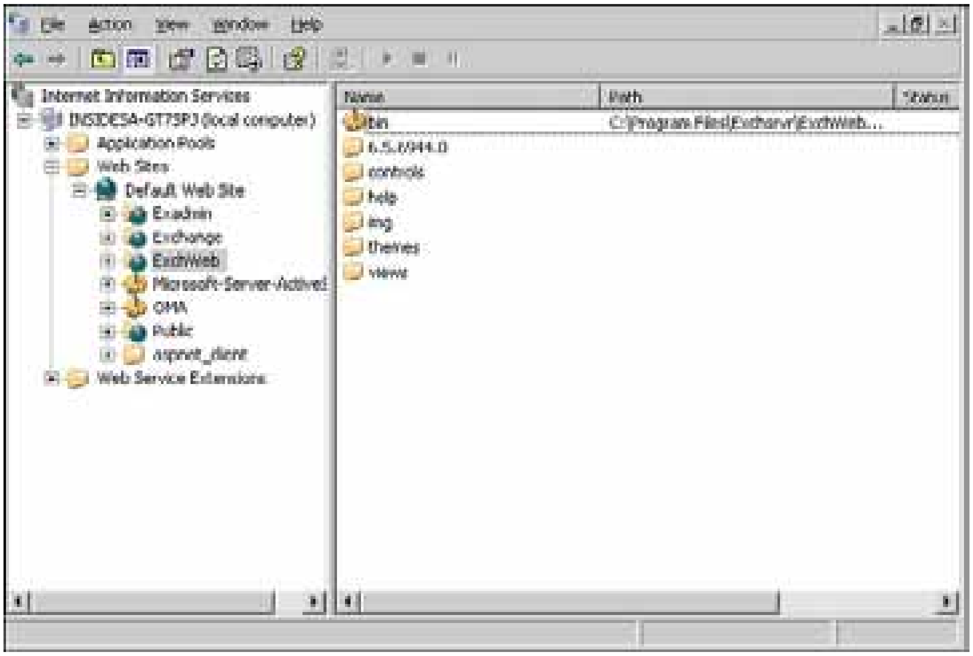
IP address: 10.0.0.1
Netmask: 255.255.255.0
Media: Auto select
Large MTU: ☑
Respond to Ping and ICMP Redirect: ☑
Trusted Subnet: ☐
Admin & Web User Login: ☑
WebMail: ☑
SNMP Agent: ☐
Centralized Management: ☐
HTTP/HTTPS Proxy: ☐

13. Click **Apply**.
    You must restart the device.

Integration with OWA 2003

OWA (Outlook Web Access) provides a way to access Exchange server mailboxes and folders through standard web browsers for platform independence. OWA 2003 is included with Microsoft Exchange 2003 server. By default, it allows all users access to their mailboxes and public folders immediately after installation with no additional configuration. The WatchGuard XCS uses an application proxy to allow users to access OWA through a secure channel.

OWA uses IIS (Internet Information Services) to access the Exchange server. Perform all configuration of directory security, authentication, and access control with the Internet Information Services Management Console (MMC) accessed in the **Administration Tools** menu of the Windows server. The *Exchweb* folder stores most of the information required to run OWA.



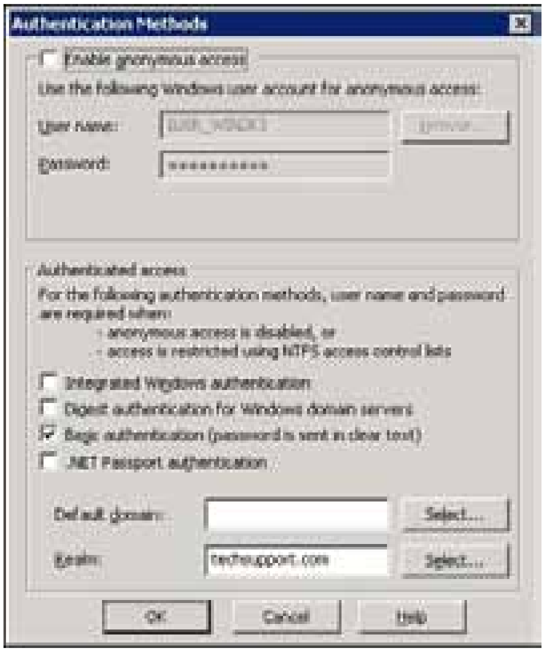
Troubleshoot Secure WebMail and OWA 2003

These sections describe certain issues that can occur when you run OWA 2003 with the Secure WebMail proxy.

Exchange Authentication

In OWA 2003, users must authenticate before they gain access to resources on the Exchange server. There are two different folders that require configuration, *Exchange* and *Exchweb*.

1. Examine the **Properties** menu of the *Exchange* folder.
2. Select **Directory Security**.
3. Select **Authentication and Access Control**.
4. Click **Edit**.



☐ Enable anonymous access

Use the following Windows user account for anonymous access:

User name: [illegible]

Password: ••••••••••

Authenticated access

For the following authentication methods, user name and password are required when:
- anonymous access is disabled, or
- access is restricted using NTFS access control lists

☐ Integrated Windows authentication

☐ Digest authentication for Windows domain servers

☑ Basic authentication (password is sent in clear text)

☐ .NET Passport authentication

Default domain:

Realm: techsupport.com

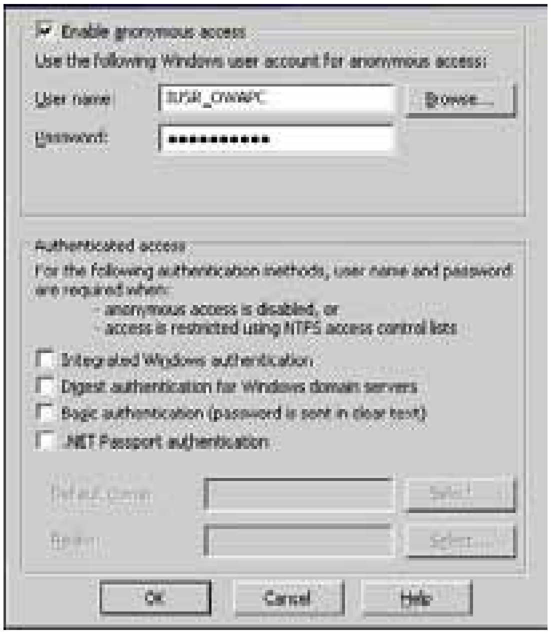
5. Make sure that **Basic Authentication** is enabled.
6. Click **OK**.

Anonymous Access

The *Exchweb* folder only requires anonymous access to allow access to webmail images.

To view the available options.

1. Examine the **Properties** menu of the *Exchweb* folder.
2. Select **Directory Security**.
3. Select **Authentication and Access Control**.
4. Click **Edit**.



☑ Enable anonymous access

Use the following Windows user account for anonymous access:

User name: IUSR_OWAPC

Password: ●●●●●●●●●●●

Authenticated access

For the following authentication methods, user name and password are required when:

- anonymous access is disabled, or
- access is restricted using NTFS access control lists

☐ Integrated Windows authentication

☐ Digest authentication for Windows domain servers

☐ Basic authentication (password is sent in clear text)

☐ .NET Passport authentication

Default domain:

Realm:

A common configuration issue that occurs when you integrate the WatchGuard XCS and OWA 2003 is that anonymous access may be turned off for the *Exchweb* folder for security reasons. After the WatchGuard XCS is installed and the Secure WebMail proxy enabled, the OWA server is not accessible.

If OWA is not accessible, you may see one of these symptoms:

5. When you log in, icons, for example, the *Inbox*, *Calendars*, *Contacts*, and *Folders*, are not displayed.
6. When you access the interface and click on any of the functions, the session logs out.

To resolve this issue, enable **Anonymous access** on the **Exchweb Authentication Methods** page.

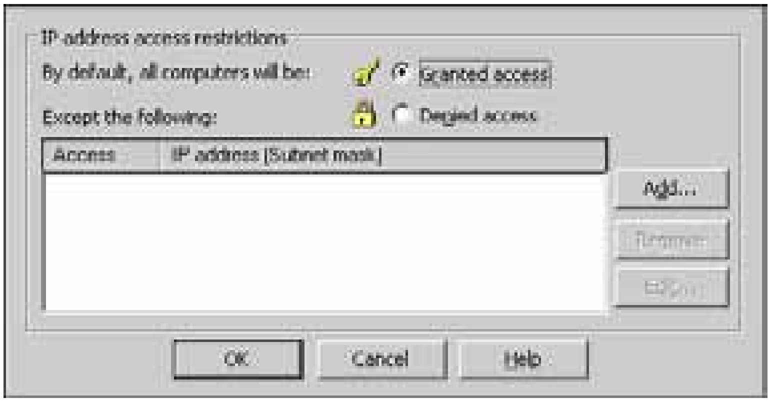
Although anonymous access seems an insecure configuration, the users have already been authenticated by the WatchGuard XCS when they log in. In this configuration, the WatchGuard XCS acts as the first point of authentication for Secure WebMail and OWA access.

IP Address and Domain Name Restrictions

You can use IIS to administer access control for hosted web sites. You can also use this feature to control access to OWA.

To configure IP address restrictions:

1. Select the **Properties** menu of the *Exchweb* folder.
2. Select **Directory Security**.
3. Select **IP Address and Domain Name Restrictions**.
4. Click **Edit**.



IP address access restrictions

By default, all computers will be: ● Granted access

Except the following: ○ Denied access

Access	IP address (Subnet mask)

5. If you enable **Granted Access**, all computers except the listed IP addresses, IP network ranges, or domain names are granted access to OWA.
6. If you enable **Denied Access**, all computers except those listed are denied access.

   When you deploy the WatchGuard XCS with OWA access, it acts on the requesting client’s behalf to establish the connection. As a result, the source IP address of the connection is the IP Address of the WatchGuard XCS device. When access control is set to deny access for the IP Address of the WatchGuard XCS, users are not able to access the OWA server properly and images on the page are not displayed.

   The web server's log displays an error code of 403 for all the image files. The log files are located in this directory:

   ```
   System root\WINNT\System32\LogFiles\W3SVC1
   ```

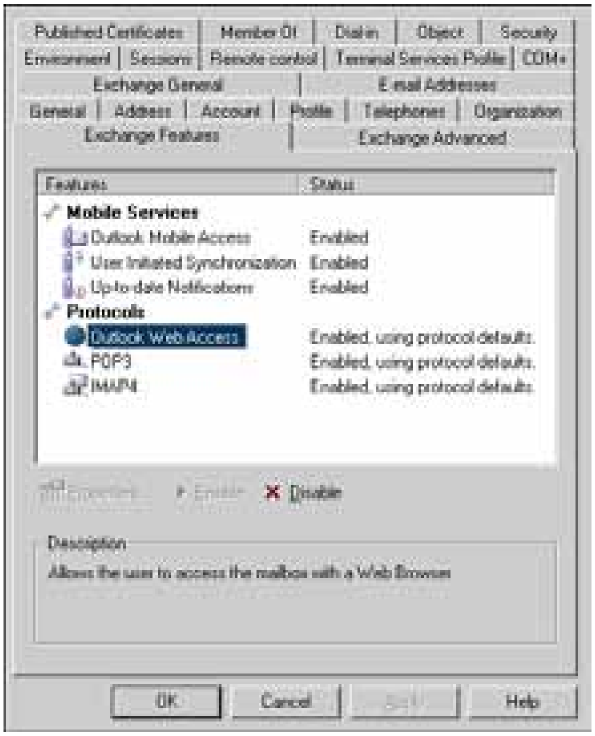
   To enable the image files, add the address of the WatchGuard XCS to the list of IP addresses that are allowed access. With these types of IP address restrictions, a typical secure configuration is to only allow access from the IP address of the WatchGuard XCS device. All users are then directed to the IP address or host name of the WatchGuard XCS for web mail access. With this configuration, all connections are secured by the WatchGuard XCS.

User Protocol Settings

You can modify each user's protocol settings to restrict or allow access to POP3, IMAP, and OWA. If you encounter issues when you access OWA, examine these settings:

To view the protocol setting for each user.

1. Open **Active Directory Users and Computers**.
2. Right-click on the user account that needs to be modified and view its properties.
3. Navigate to the **Exchange Features** tab.
   You can only access this menu if you enable the **View > Advanced Features** *option.*



Features	Status
Mobile Services	
Outlook Mobile Access	Enabled
User Initiated Synchronization	Enabled
Up-to-date Notifications	Enabled
Protocols	
Outlook Web Access	Enabled, using protocol defaults.
POP3	Enabled, using protocol defaults.
IMAP4	Enabled, using protocol defaults.

Description

Allows the user to access the mailbox with a Web Browser

4. Make sure you enable **Outlook Web Access** in the **Protocols** section.

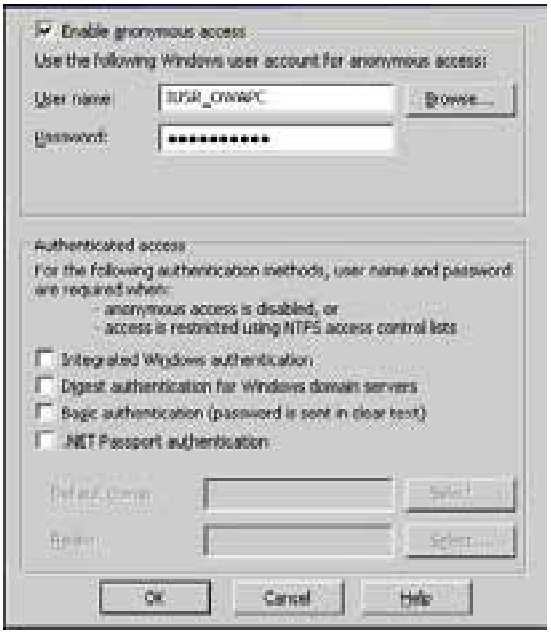
   If you do not enable this option, logging in to the OWA server through the WatchGuard XCS results in the “HTTP/1.0 403 Forbidden” error.

Local NTFS Permissions

The WatchGuard XCS only supports anonymous access. The Exchange account that is used for anonymous access must have the appropriate permissions to access local Exchange resources.

To configure the permissions:

1. In the IIS configuration, right-click on the *Exchweb* folder.
2. Select **Properties**.
3. Select **Directory Security**.
4. Select **Authentication and Access Control**.
5. Click **Edit**.



☑ Enable anonymous access

Use the following Windows user account for anonymous access:

User name: IUSR_OWAPC

Password: ●●●●●●●●●●●

Authenticated access

For the following authentication methods, user name and password are required when:

- anonymous access is disabled, or
- access is restricted using NTFS access control lists

☐ Integrated Windows authentication

☐ Digest authentication for Windows domain servers

☐ Basic authentication (password is sent in clear text)

☐ .NET Passport authentication

Default domain:

Realm:

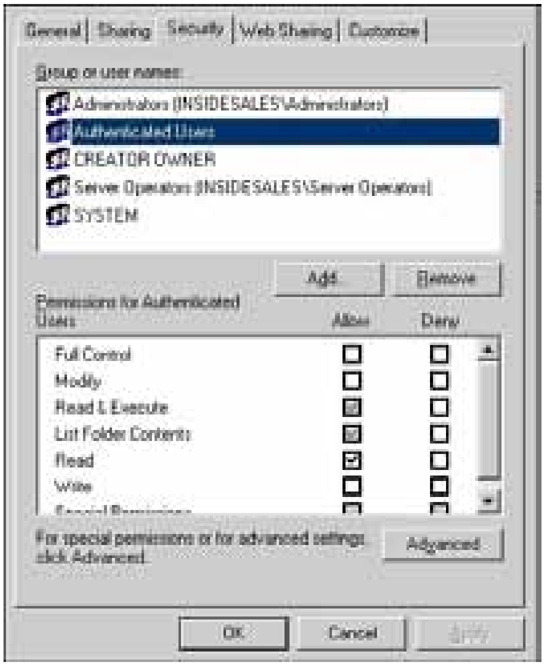
6. The default account used for anonymous access must be IUSR_<computer name>.

   If the computer name is OWAPC, the user account is IUSR_OWAPC. Make sure that this user has permissions for this directory:

   ```
   System Root\Program Files\Exchsrvr\exchweb
   ```

7. Right-click on the directory and select **Properties**.
8. Select the **Security** tab.
9. Make sure that the **Authenticated Users** group has **Read & Execute**, **List Folder Contents**, and **Read** permissions set to **Allow**.

   The Authenticated Users group includes the anonymous user (IUSR_<computer name>) as specified by IIS.



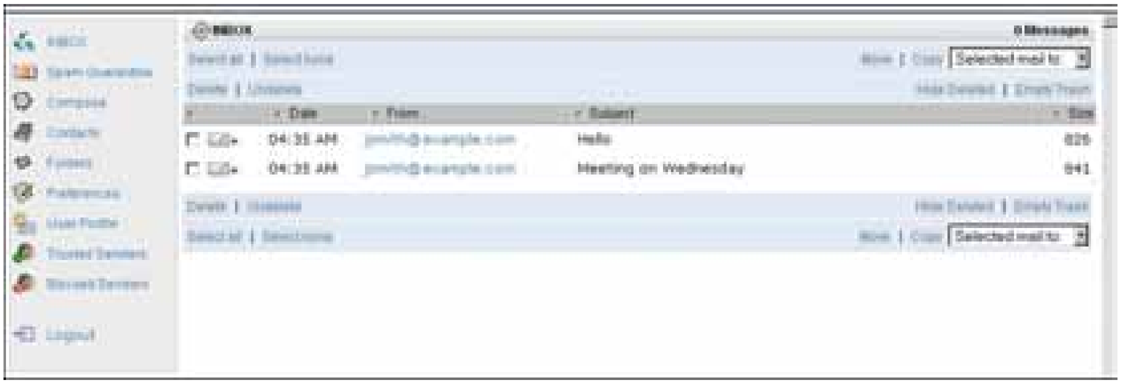
Administrators (INSIDESALES\Administrators)
Authenticated Users
CREATOR OWNER
Server Operators (INSIDESALES\Server Operators)
SYSTEM

Permissions for Authenticated Users	Allow	Deny
Full Control	□	□
Modify	□	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	□	□
Special Permissions	□	□

WebMail Client

Use the WebMail client to access local mailboxes, IMAP Servers, administrative access, the User Spam Quarantine, and the Trusted/Blocked Senders List. WebMail logins are authenticated as local users or remote LDAP and RADIUS users.

From a web browser, type the host name or IP address of the WatchGuard XCS system that runs WebMail. Log in with your local or LDAP/RADIUS User ID and password. After you successfully log in, the WebMail interface appears.

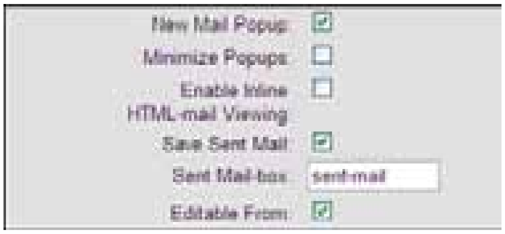


#	Date	From	Subject	Size
□	04:35 AM	jsmith@example.com	Hello	826
□	04:35 AM	jsmith@example.com	Meeting on Wednesday	841

Configure WebMail Client Options

To configure WebMail Client options:

1. Select **Configuration > WebMail > WebMail**.
2. Go to the **WebMail Options** section.



New Mail Popup: ☑

Minimize Popups: □

Enable Inline HTML-mail Viewing: □

Save Sent Mail: ☑

Sent Mail-box: sent-mail

Editable From: ☑

3. To enable a popup window for new mail notification, select the **New Mail Popup** check box.
   To see popup windows, you must enable popups on your web browser.
4. To minimize the use of new popup browser windows and use the main frame, select the **Minimize Popups** check box.
5. To enable the ability to view HTML mail, select the **Enable Inline HTML-mail Viewing** check box.
   For security reasons, any scripts and fetches for external objects are filtered.
6. To enable the ability to save sent mail in the user's mailbox, select the **Save Sent Mail** check box.
7. In the **Sent Mail-box** text box, type the name to use for the sent mail folder if you enable this feature.
8. To allow a user to edit the From: field when they compose a message, select the **Editable From** check box.
9. Click **Apply**.

16 Threat Prevention

About Threat Prevention

The Threat Prevention feature detects and mitigates incoming threats. When you enable the default Threat Prevention configuration, the WatchGuard XCS can recognize these threats:

- Directory harvesting
- Denial of Service (DoS) attacks
- Connections from blocked addresses
- Connections originating from addresses that send spam
- Connections originating from addresses that send viruses

The WatchGuard XCS retains historical information about connecting IP addresses and how they behave. You can accept or reject a connection at connection time based on this current and historical data.

You can also push this information to a perimeter F5® or Cisco® device that can rate limit, throttle or block a given IP address for a period of time before it reaches the WatchGuard XCS.

How Threat Prevention Works

The Threat Prevention feature performs these tasks:

- Determines the threat level of connecting IP addresses and retains historical statistics about that address
- Acts on the connection’s IP address based on its connection history
- The Threat Prevention feature is involved in these stages of mail delivery for a specific client IP address:
- At connection request time, the WatchGuard XCS provides the history for the IP address to the rules script that determines if the connection is allowed or rejected. It also identifies how to further classify the address into a specific data group.
- After early mail scanning, the WatchGuard XCS adds the number of known recipients, unknown recipients, and DNSBL results to the history of the connecting address.

- After full mail scanning, the WatchGuard XCS records the results of Anti-Virus, Anti-Spam, and Malformed message scanning in the history for the IP address.
- Prior to connection, an F5 or Cisco device (if configured) can block an IP address before it reaches the WatchGuard XCS.

Threat Prevention in a Cluster

When you use the Threat Prevention feature in a cluster, you only need to configure it on the Primary device of the cluster. The Primary is the only point of contact between the cluster and any configured load balancing devices.

> **Note** *Threat Prevention decisions are based on per system statistics, and not on statistics for the entire cluster.*

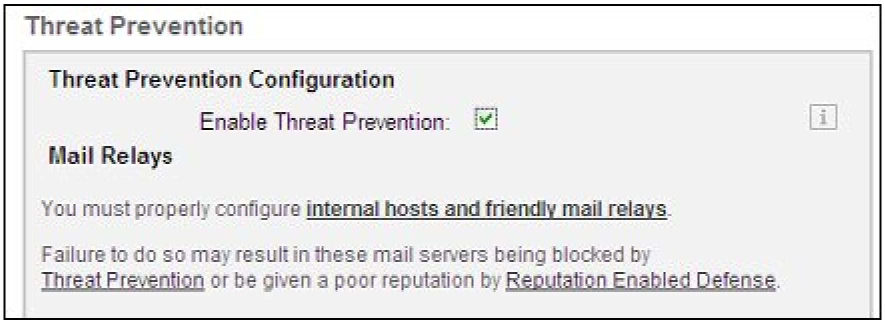
If you demote a Primary cluster device, and promote a Secondary to be Primary, the cluster switches control and resynchronizes to the load balancing device. Threat Prevention runs independently on each device in the cluster, but only the Primary pushes data to the external devices.

Configure Threat Prevention

A Connection Rules script runs each time a client tries to connect to the WatchGuard XCS. This configurable. script determines whether to accept or reject a connection based on the threat prevention history of the IP address. The script is also responsible for moving IP addresses into appropriate data groups.

To configure Threat Prevention:

1. Select **Security > Anti-Spam > Threat Prevention > Configure**.
   The Threat Prevention page appears.



Threat Prevention

Threat Prevention Configuration

Enable Threat Prevention: ☑

Mail Relays

You must properly configure internal hosts and friendly mail relays.

Failure to do so may result in these mail servers being blocked by Threat Prevention or be given a poor reputation by Reputation Enabled Defense.

2. Select the **Enable Threat Prevention** check box.
   The default connection rules immediately take effect.

> **Note** *Examine and customize (if required) the default connection rules before you enable Threat Prevention.*

Mail Relays

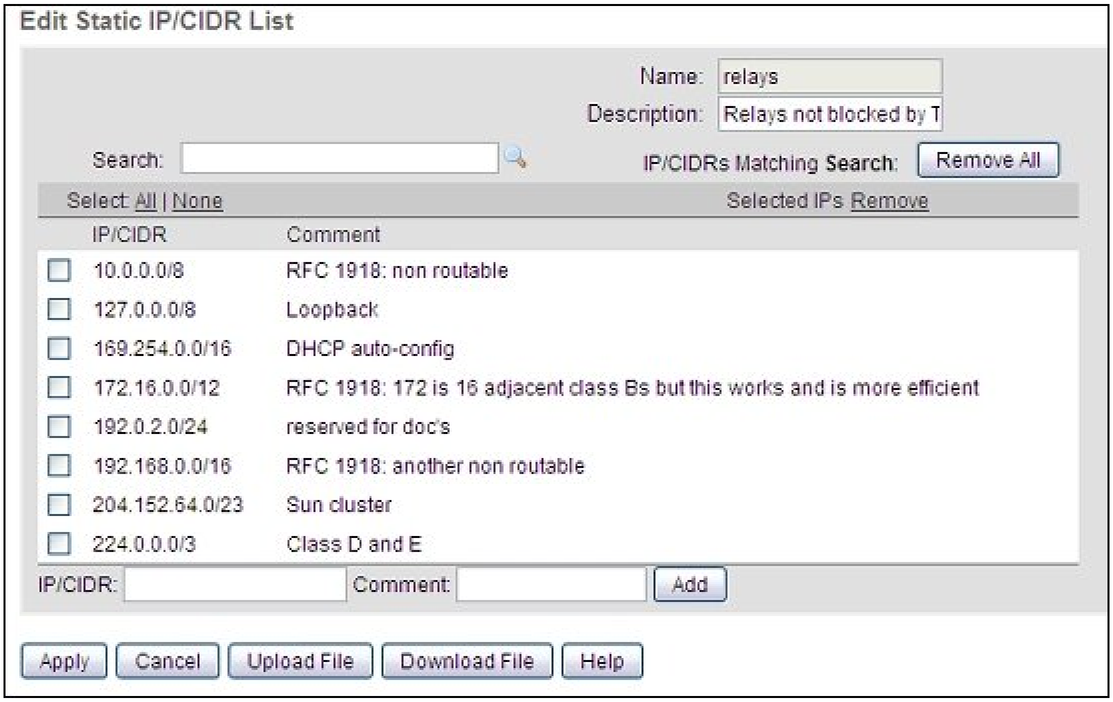
You can trust friendly local networks or addresses of known mail servers in your environment that relay mail through the WatchGuard XCS. You can add these specific networks and servers to the relays IP/CIDR list in the Threat Prevention configuration to prevent the Threat Prevention and Reputation Enabled Defense features from blocking them, as well as to make sure that reputation statistics for these addresses are not reported to the Reputation Enabled Defense service.

For example, it is possible that in environments with a backup MTA (Mail Transfer Agent), the backup can be blocked by Threat Prevention rules or improperly classified by Reputation Enabled Defense. If the primary WatchGuard XCS is offline, mail is collected by the backup MTA as specified in your organization's DNS MX records.

When the primary WatchGuard XCS comes back online, this mail (that can include spam, viruses, and other types of infected mail) from the backup MTA is forwarded to the WatchGuard XCS for processing. Because of this mail, the backup MTA can be blocked Threat Prevention, or receive a low reputation score by Reputation Enabled Defense.

To add a server to the relays list:

1. Select **Security > Anti-Spam > Threat Prevention > Configure**.
2. Click **internal hosts and friendly mail relays**.
   The relays static IP/CIDR list page appears.



Edit Static IP/CIDR List

Name: relays
Description: Relays not blocked by T

Search:
IP/CIDRs Matching Search: Remove All

Select: All | None   Selected IPs Remove

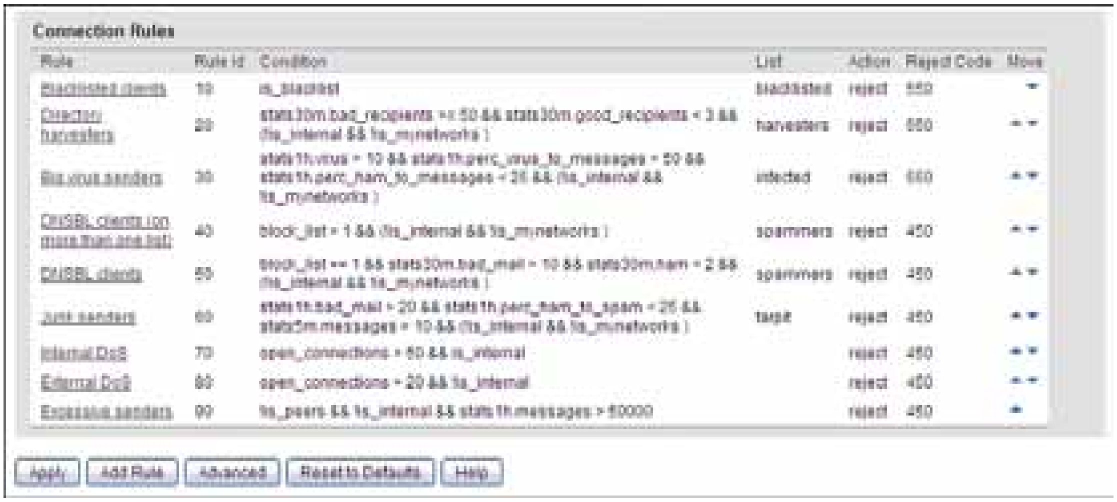
	IP/CIDR	Comment
□	10.0.0.0/8	RFC 1918: non routable
□	127.0.0.0/8	Loopback
□	169.254.0.0/16	DHCP auto-config
□	172.16.0.0/12	RFC 1918: 172 is 16 adjacent class Bs but this works and is more efficient
□	192.0.2.0/24	reserved for doc's
□	192.168.0.0/16	RFC 1918: another non routable
□	204.152.64.0/23	Sun cluster
□	224.0.0.0/3	Class D and E

IP/CIDR: Comment: Add

3. Add the address of any internal relays and a description.
4. Click **Add**.
5. Click **Apply**.

About Connection Rules

Threat Prevention uses a scripting language for connection rule checks that drive the decision process. The script can reject or accept mail based on various statistics available at the time of client connection. The listed default rules are processed in order.



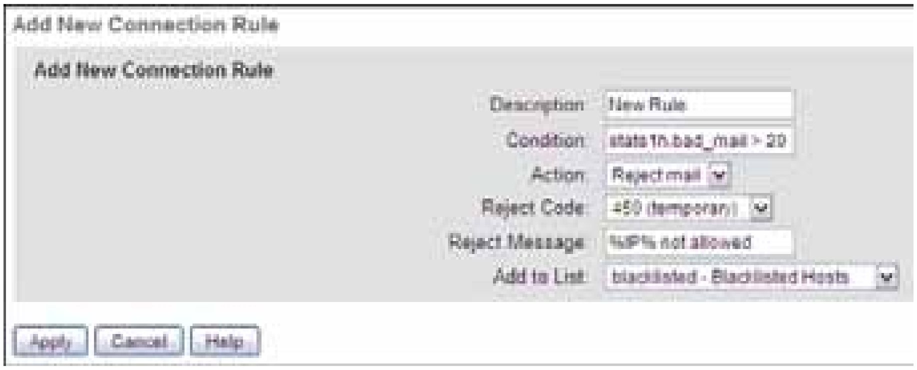
Connection Rules

Rule	Rule id	Condition	List	Action	Reject Code	Move
Blacklisted clients	10	is_blacklist	blacklisted	reject	550	▼
Directory harvesters	20	stats30m.bad_recipients >= 50 && stats30m.good_recipients < 3 && (!is_internal && !is_mynetworks)	harvesters	reject	550	▲▼
Big virus senders	30	stats1h.virus > 10 && stats1h.perc_virus_to_messages > 50 && stats1h.perc_ham_to_messages < 25 && (!is_internal && !is_mynetworks)	infected	reject	550	▲▼
DNSBL clients (on more than one list)	40	block_list > 1 && (!is_internal && !is_mynetworks)	spammers	reject	450	▲▼
DNSBL clients	50	block_list == 1 && stats30m.bad_mail > 10 && stats30m.ham < 2 && (!is_internal && !is_mynetworks)	spammers	reject	450	▲▼
Junk senders	60	stats1h.bad_mail > 20 && stats1h.perc_ham_to_spam < 25 && stats5m.messages > 10 && (!is_internal && !is_mynetworks)	tarpit	reject	450	▲▼
Internal DoS	70	open_connections > 50 && is_internal		reject	450	▲▼
External DoS	80	open_connections > 20 && !is_internal		reject	450	▲▼
Excessive senders	90	!is_peers && !is_internal && stats1h.messages > 50000		reject	450	▲

- **Rule** – A descriptive name for the rule.
- **Rule ID** – The ID number associated with the rule.
- **Condition** – Condition statement to execute. Condition statements are described in detail in the next section.
- **List** – Defines which list to insert the IP address.
- **Action** – Action to take if the condition is “true”, for example, **Accept** or **Reject**.
- **Reject Code** – Reply code to send to the connecting client.
- For **Reject**, this is “450 (temporary)” or “550 (permanent)”.
- For **Accept**, the reply code is set to “220 (OK)”.
- **Move** – Use the arrow icons to modify the processing order of the connection rules.

To add a new connection rule:

1. Click **Add Rule**.



Add New Connection Rule

Add New Connection Rule

Description:	New Rule
Condition:	stats1h.bad_mail > 20
Action:	Reject mail
Reject Code:	450 (temporary)
Reject Message:	%IP% not allowed
Add to List:	blacklisted - Blacklisted Hosts

2. Click **Apply**.
   The script is automatically checked for syntax and execution errors.

3. Click **Advanced** to view the entire connection rules script based on the configured rules.

Rules Script

The Threat Prevention feature runs a connection rules script each time a client connects to the WatchGuard XCS. The script determines whether to accept or reject a connection based on its threat prevention history. The script is also responsible for moving IP addresses into appropriate data groups, for example, *infected* or *spammers*. You cannot edit the full script, but you can define rules that are updated in the script.

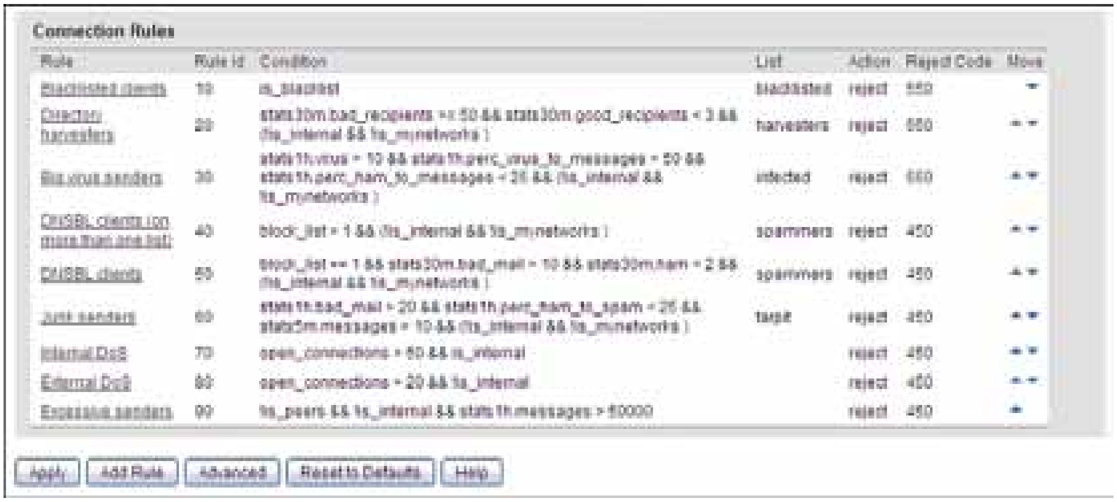
Basic Rule Structure

The basic structure of a connection rule is:

- **Rule Condition** – A set of criteria that must be met for the rule to trigger, for example, “stats1h.virus > 10” (10 or greater virus-infected messages sent in the last hour). Threat Prevention collects over fifteen different types of data that you can use to create a rule condition.
- **Action** – Action to take when the rule condition is true, for example, **Accept** or **Reject**.
- **Reject code** – The reject code to send back to the sending server, for example, **temporary reject (450)** or **permanent reject (550)**.
- **List** – The data group to which to add this IP address, if the condition is true. For example, a sender that triggers a spam rule is placed in the *spammers* group.

Default Connection Rules

The default connection rules are active when you enable Threat Prevention. These rules include checks for typical conditions, for example, blocked clients, virus and junk mail senders, and denial of service (DoS) attempts. The default rules are also helpful for learning how to put together condition statements for your own custom connection rules.



Connection Rules

Rule	Rule Id	Condition	List	Action	Reject Code	Move
Blacklisted clients	10	is_blacklist	blacklisted	reject	550	▼
Directory harvesters	20	stats30m.bad_recipients >= 50 && stats30m.good_recipients < 3 && (!is_internal && !is_mynetworks)	harvesters	reject	550	▲▼
Big virus senders	30	stats1h.virus > 10 && stats1h.perc_virus_to_messages > 50 && stats1h.perc_ham_to_messages < 25 && (!is_internal && !is_mynetworks)	infected	reject	550	▲▼
DNSBL clients (on more than one list)	40	block_list > 1 && (!is_internal && !is_mynetworks)	spammers	reject	450	▲▼
DNSBL clients	50	block_list == 1 && stats30m.bad_mail > 10 && stats30m.ham < 2 && (!is_internal && !is_mynetworks)	spammers	reject	450	▲▼
Junk senders	60	stats1h.bad_mail > 20 && stats1h.perc_ham_to_spam < 25 && stats5m.messages > 10 && (!is_internal && !is_mynetworks)	tarpit	reject	450	▲▼
Internal DoS	70	open_connections > 50 && is_internal		reject	450	▲▼
External DoS	80	open_connections > 20 && !is_internal		reject	450	▲▼
Excessive senders	90	!is_peers && !is_internal && stats1h.messages > 50000		reject	450	▲

Blacklisted Clients

This rule checks to see if the client is already blocked by Threat Prevention. The condition statement "is_ blacklist" checks if the client is listed in the *blacklist* IP/CIDR list. The client is rejected and added to the *blacklisted* data group if the condition is true.

Directory Harvesters

This rule checks whether the client has been involved with directory harvesting activities intended to discover valid email addresses from the WatchGuard XCS. This condition statement is used to identify if a client is considered a directory harvester:

```
stats30m.bad_recipients >= 50 && stats30m.good_recipients < 3 && (!is_internal &&
!is_mynetworks)
```

This statement checks these conditions:

- the number of invalid recipients from the client in the last 30 minutes is greater than or equal to 50
- the number of good recipients from the client in the last 30 minutes is less than 3
- the client does not exist in the *internal* or *mynetworks* IP/CIDR lists (to trust the client)

If all the conditions are true, then reject the connection and add its IP address to the *harvesters* data group

Big Virus Senders

This rule checks whether the client has recently sent a large number of viruses. This condition statement is used to identify whether the client is considered a source of viruses:

```
stats1h.virus > 10 && stats1h.perc_virus_to_messages > 50 && stats1h.perc_ham_to_
messages < 25 && (!is_internal && !is_mynetworks)
```

This statement checks these conditions:

- the number of viruses received from this client in the last hour is greater than 10
- the percentage of virus infected messages received from this client in the last hour is greater than 50
- the percentage of clean messages received from this client in the last hour is less than 25
- the client does not exist in the *internal* or *mynetworks* IP/CIDR lists (to trust the client)

If all the conditions are true, then reject the connection and add its IP address to the *infected* data group

DNSBL Clients (on more than one list)

This rule checks whether the client has been listed on more than one DNS Block List of blocked clients. If the client is on more than one DNSBL, it is considered a known open-relay that sends out a large number of spam messages. This condition statement is used to identify whether the client is on more than one DNSBL:

```
block_list > 1 && (!is_internal && !is_mynetworks)
```

This statement checks these conditions:

- the client exists on more than one DNSBL
- the client does not exist in the *internal* or *mynetworks* IP/CIDR lists (to trust the client)

If all the conditions are true, then temporarily reject the connection and add its IP address to the *spammers* data group.

DNSBL Clients

This rule checks whether the client exists on only one DNS Block List. In this case, there is the possibility that the client is on this DNSBL by mistake, and the WatchGuard XCS makes additional checks to examine its recent history of mail messages. This condition statement is used to identify whether a client is on one DNSBL and sends a large number of spam messages:

```
block_list == 1 && stats30m.bad_mail > 10 && stats30m.ham < 2 && (!is_internal &&
!is_mynetworks)
```

This statement checks these conditions:

- the client exists on only one DNSBL
- the number of spam and junk messages received from this client in the last 30 minutes is greater than 10
- the number of clean messages received from this client in the last 30 minutes is less than 2
- the client does not exist in the *internal* or *mynetworks* IP/CIDR lists (to trust the client)

If all the conditions are true, then temporarily reject the connection and add its IP address to the *spammers* data group.

Junk Senders

This rule checks whether the client sends out a large amount of spam or junk mail in proportion to the number of legitimate messages. This condition statement is used to identify whether a client is sending a large amount of spam or junk messages, as compared to legitimate messages:

```
stats1h.bad_mail > 20 && stats1h.perc_ham_to_spam < 25 && stats5m.messages > 10 &&
(!is_internal && !is_mynetworks)
```

This statement checks these conditions:

- the number of spam and junk messages received from this client in the last hour is greater than 20
- the percentage of clean messages compared to spam received from this client in the last hour is less than 25
- the number of messages sent from this client in the last five minutes is greater than 10
- the client does not exist in the *internal* or *mynetworks* IP/CIDR lists (to trust the client)

If all the conditions are true, then temporarily reject the connection and add its IP address to the *tarpit* data group.

Internal DoS

This rule checks whether the client is on an internal network and is using a lot of open connections that may result in a denial of service. This condition statement is used to identify whether an internal client is creating a large amount of open connections:

```
open_connections > 50 && is_internal
```

This statement checks these conditions:

- the number of open connections from this client is greater than 50
- the client is listed in the *internal* IP/CIDR list

If all the conditions are true, then temporarily reject the connection.

External DoS

This rule checks whether an external client is using a lot of open connections that can result in a denial of service. This condition statement is used to identify whether an external client is creating a large amount of open connections:

```
open_connections > 20 && !is_internal
```

This statement checks these conditions:

- the number of open connections from this client is greater than 20
- the client is not listed in the *internal* IP/CIDR list

If all the conditions are true, then temporarily reject the connection.

Excessive Senders

This rule checks whether a client is sending too many messages that can result in a denial of service. This condition statement is used to identify whether a client is sending an abnormal amount of messages:

```
!is_peers && !is_internal && stats1h.messages > 50000
```

This statement checks these conditions:

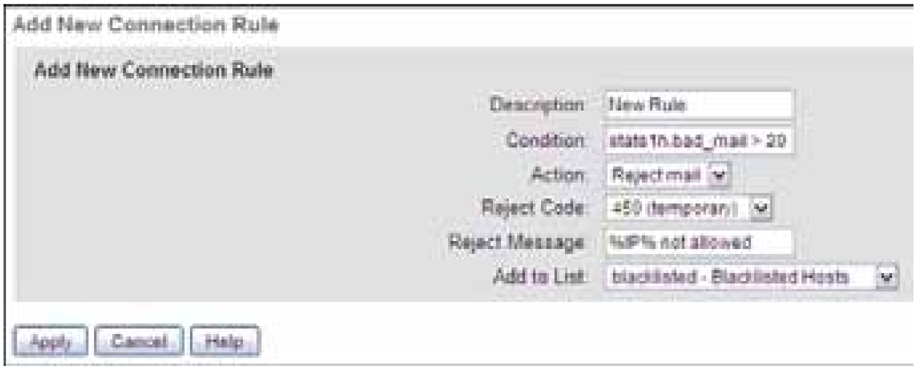
- the client is not listed in the *peers* and *internal* IP/CIDR lists (to trust the client)
- the number of messages sent from this client in the last hour is greater than 50000

If all the conditions are true, then temporarily reject the connection.

Create Connection Rules

To create custom connection rules:

1. Select **Security > Anti-Spam > Threat Prevention**.
2. Click **Add Rule**.
   The Add New Connection Rule page appears.



Add New Connection Rule

Add New Connection Rule

Description: New Rule
Condition: stats1h.bad_mail > 20
Action: Reject mail
Reject Code: 450 (temporary)
Reject Message: %IP% not allowed
Add to List: blacklisted - Blacklisted Hosts

You can configure these options:

- **Description** – Type a descriptive summary of the rule.
- **Condition** – Type a condition statement to execute.

For example:

```
stats1h.bad_mail > 20 && (!is_internal && !is_mynetworks)
```

This statement checks whether the client has sent more than 20 virus-infected or spam messages in the last hour, and is not on the *internal* or *mynetworks* IP address lists.

See *Build Condition Statements* for detailed information on creating custom statements.

- **Action** – Action to take if the condition is true. Options are **Accept Mail** or **Reject Mail**.
- **Reject Code** – Reply code to send to the connecting client. For **Reject Mail**, this is “450 (temporary)” or “550 (permanent)”. For **Accept Mail**, the reply code is set to “220 (OK)”.
- **Reject Message** – A customized reject message to send to the connecting client. The %IP% variable can be used to include the IP address of the client in the message.
- **Add to List** – Select a data group to which to add the client IP address if the condition is true. View and configure these lists in **Security > Anti-Spam > Threat Prevention > Data Groups**.

3. Click **Apply**.

Build Condition Statements

The Threat Prevention rules are based on condition statements that define various criteria for the connecting clients and their historical behavior. These tables describe the variables, parameters, and Boolean operators available to create Threat Prevention rules.

General Statistics

These are general statistics that you can use when you create connection rules. These include items, for example, the IP address of the connecting client, and how many open connections a client is using.

Statistic	Description
ip_address	The IP address of the connecting client.
current_group	The name of the current data group the client IP addresses is in, if any.
open_connections	The current number of open connections to this IP address.
block_list	If DNS Block lists are enabled, this indicates the number of lists the IP address is on.
rule_no	Indicates the connection rule number for ordering purposes.

For example, as part of your condition statement to prevent denial of service attacks, you can check that the client does not have a large amount of open connections with this statement:

```
open_connections > 50
```

IP Lists

These parameters identify whether the client IP address is listed in any of the pre-defined IP lists (defined in **Security > Anti-Spam > Threat Prevention > IP/CIDR Lists**).

This allows you to check if the client IP address is trusted because it is identified as an internal system, a network under your control, or a peer address. The client can also be blocked if it appears in the local blacklist.

IIP/CIDR List	Description
is_internal	Checks if the client IP address is listed in the *internal* address list.
is_mynetworks	Checks if the client IP address is listed in the *mynetworks* address list.
is_peers	Checks if the client IP address is listed in the *peers* address list.
is_blacklist	Checks if the client IP address is listed in the *blacklisted* address list.

For example, to check if the connecting client is in the *blacklist* IP/CIDR list, use this condition statement:

```
is_blacklist
```

If the client is already listed in the *blacklist* IP list, the condition is true and the configured action executed.

You can use these to make sure that clients are trusted because they are considered internal or under an organization's control. For example, to check for a large amount of open connections, and to make sure this client is not an internal client, use this statement:

```
open_connections > 50 && !is_internal
```

This statement checks clients who have more than 50 open connections and do not belong to the *internal* IP/CIDR list.

Email Statistics

These email statistics can be used to build condition statements in the connection rules based on the types of messages received. These statistics identify the number of messages based on their classification, for example, virus-infected, malformed, spam, and clean. Several statistics also indicate the percentage of one type of message to another, for example, the percentage of spam messages to total messages received.

Email Statistic	Description
messages	Total number of messages from successful connections.
virus	Number of virus-infected messages.
malformed	Number of malformed messages.
spam	Number of spam messages (Intercept Certainly Spam or Probably Spam, Brightmail spam, and Pattern Filter spam).

Email Statistic	Description
ham	Number of messages that are clean (not spam, virus, or malformed).
connection_attempts	Number of attempted connection attempts.
bad_mail	Number of viruses, malformed, and spam messages.
bad_recipients	Number of unknown recipients (or 0 if the *Reject on unknown recipient* feature is disabled).
good_recipients	Number of legitimate recipients.
perc_ham_to_messages	Percentage of clean messages to the total amount of messages.
perc_virus_to_messages	Percentage of virus-infected messages to the total amount of messages.
perc_spam_to_messages	Percentage of spam messages to the total amount of messages.
perc_malformed_to_messages	Percentage of malformed messages to the total amount of messages.
perc_bad_to_messages	Percentage of bad messages (virus, malformed, and spam) to the total amount of messages.
perc_ham_to_spam	Percentage of clean messages to the total amount of spam messages.

These email statistics must be used in combination with a specific time period. This allows you to check for the number of certain types of email messages, for example, spam messages, in a certain time period, for example, 24 hours.

This table describes various time periods that you can use in conjunction with the email statistics variables.

Time Period	Description
stats1m	Statistics for the last minute.
stats5m	Statistics for the last 5 minutes.
stats15m	Statistics for the last 15 minutes.
stats30m	Statistics for the last 30 minutes.
stats1h	Statistics for the last hour.
stats24h	Statistics for the last 24 hours (1 day).

Specify the time period and the email statistics parameter separated by a "." (period). For example, to check how many spam messages were received in the last 24 hours, use this statement:

```
stats24h.spam
```

To check the percentage of the number of spam messages compared to the total amount of messages in the last hour, use this statement:

```
stats1h.perc_spam_to_messages
```

Boolean Operators and Syntax

These are the Boolean operators that you can sue when building condition statements. To combine operators, use this syntax, `(a && (b || c))`. This produces the result: a AND (b OR c).

Boolean Operator	Description
&&	and
!	not
||	or
>	Greater than
<	Less than
==	Equal to
>=	Greater than or equal to
<=	Less than or equal to

For example, to make sure a host is not listed in the *internal* and *mynetworks* IP/CIDR lists (to trust the system for Threat Prevention), use this statement:

```
!is_internal && !is_mynetworks
```

This example shows how to use multiple Boolean operators to combine condition statements:

```
stats30m.bad_recipients >= 50 && stats30m.good_recipients < 3
```

This example checks the number of good and bad recipients in the last 30 minutes. If the bad recipients are greater than or equal to 50, and the good recipients are less than 3, then the condition is true.

Connection Rules Script Error Check

When you are finished with the changes and additions to the connection rules, click **Apply**. The results of the script test are displayed. This includes any syntax errors if they occur. If an error occurs, examine the rule you just applied and check the condition statement to make sure that it conforms to the proper syntax and that you correctly entered any variables or parameters.

IP/CIDR Lists

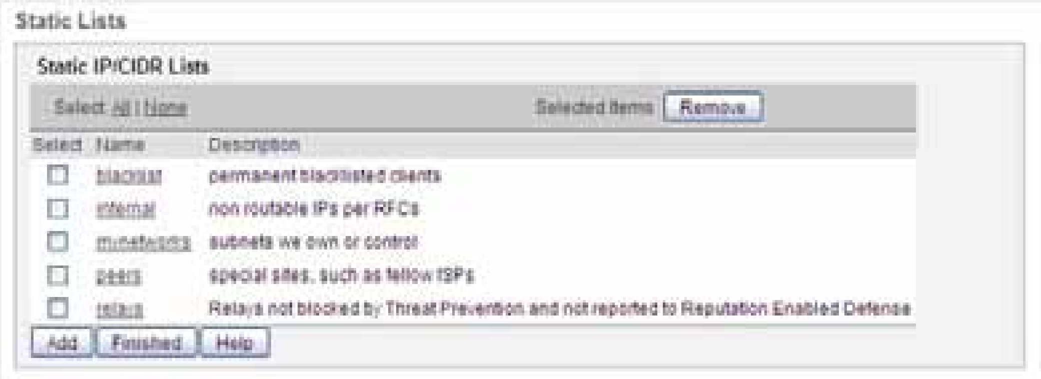
Use *IP/CIDR address lists* to define specific groups of IP addresses that affect Threat Prevention processing. When a client connects, the connection rules script looks up the client's IP address in the existing IP/CIDR lists and performs any defined actions for that list. This allows you to trust, block, or provide additional classification for a specific IP address or subnet.

For example, if the address is listed in the *blacklist*, the connection rules script rejects the message. Addresses in the *peers* or *mynetworks* list are exempted from some of the checks because they are known sources or internal networks of your organization.

It is critical that you add any non-routable networks that you use locally to the *internal* address list and make sure any networks under your organization's control or friendly networks are listed in the *mynetworks* and *peers* list respectively. This prevents any local addresses from being blocked by Threat Prevention processing.

To configure IP/CIDR lists:

1. Select **Security > Anti-Spam > Threat Prevention > IP/CIDR Lists**.
   The Static IP/CIDR Lists page appears.



Static Lists

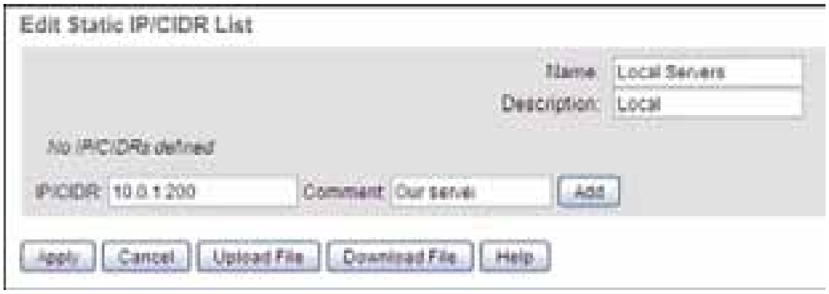
Static IP/CIDR Lists

Select: All | None   Selected Items: Remove

Select	Name	Description
□	blacklist	permanent blacklisted clients
□	internal	non routable IPs per RFCs
□	mynetworks	subnets we own or control
□	peers	special sites, such as fellow ISPs
□	relays	Relays not blocked by Threat Prevention and not reported to Reputation Enabled Defense

- **blacklist** – List of any IP addresses or networks from which you do not want to receive email.
- **internal** – List of internal non-routable IP addresses from which you always accept mail, for example, the 192.168.0.0 network.
- **mynetworks** – A list of networks and subnets under your organization's control from which you always accept mail.
- **peers** – A list of special sites, for example, peer ISP networks from which you typically accept mail.
  The peers list is not used by the default connection rules. You must modify the current rules or add a new connection rule to use this list.
- **relays** – A list of mail servers that need to relay mail through this WatchGuard XCS. This prevents these servers from being blocked by content-based Threat Prevention rules and Reputation Enabled Defense, as well as being reported to the Reputation Enabled Defense service.

2. Click **Add**.



Edit Static IP/CIDR List

Name: Local Servers
Description: Local

No IP/CIDRs defined

IP/CIDR: 10.0.1.200   Comment: Our server

3. In the **Name** text box, type a name for this list.
   This text box cannot be left blank, and must consist of only alphanumeric characters.
4. In the **Description** text box, type a description for this address list.
5. In the **IP/CIDR** text box, type one of these address types:
6. Single IP address, for example, `192.168.1.125`
7. Subnet in CIDR format, for example, `192.168.0.1/24`
8. Class A, B, or C subnet with trailing octets removed, for example, `192.168`
9. In the **Comment** text box, type a descriptive comment to describe the address in this list.
10. Click **Add**.
11. Click **Apply**.

Upload and Download IP Addresses

You can upload a list of list addresses in one text file. The file must contain comma or tab separated entries. Use this format:

```
[address],[description]
```

For example:

```
192.168.0.0/16,non-routable
```

You must use a text editor to create the file ipcidr.csv.

To update a list file:

1. To download the list from the WatchGuard XCS, click **Download File**.
2. Open the file and update the list.
3. Click **Upload File** and upload the edited file to the WatchGuard XCS.

Data Groups

Threat Prevention places IP addresses into *Data Groups* for a specified period of time and sets the response to connection requests for clients who are in these groups. You can configure data groups to perform a specific action (for example, “450 temporary reject” or “550 permanent reject”) and a time period to execute that action.

Data groups differ from IP/CIDR lists because their contents are always changing based on the latest threat prevention data. Use IP/CIDR lists to define trusted and blocked lists based on addresses specific to your organization. Data groups build their data from the history of connecting addresses, and assign specific rules and actions to these addresses based on that history.

The Threat Prevention connection rules script adds IP addresses to these lists if they match a specific behavior. For example, messages from an IP address that indicate harvesting of email addresses are moved into the *harvesters* list. When that same IP address tries to connect again after being added to the list, it is rejected with a configured reject code for the list if it is configured with the reject action.

For example, the *harvesters* list rejects with the code “550 denied due to too many unknown recipients”. No further statistics are gathered on that IP address during this early reject period and further Threat Prevention rules do not apply. The data group releases the IP address after a configurable period of time. Data groups can contain tens of thousands of IP addresses.

Data groups with an action of **Just Log** pass the request on to the rules processing script. The rules script can then specify its own reject or accept action. If the rules script specifies an accept action, further statistics are gathered as the mail is received and processed.

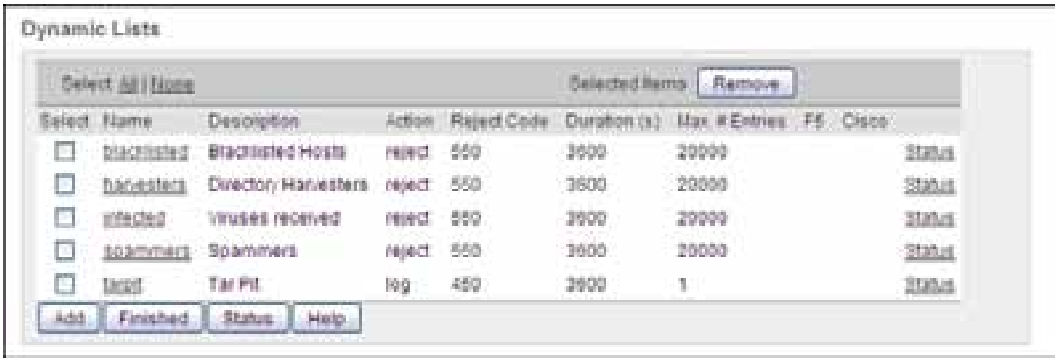
Integration with F5 and Cisco Devices

You can also push the contents of data groups to a perimeter F5 or Cisco device. This allows the F5 or Cisco device to process connections from the IP address and to act accordingly before the connection reaches the WatchGuard XCS.

Configure Data Groups

To configure data groups:

1. Select **Security > Anti-Spam > Threat Prevention > Data Groups**.
   The Dynamic Lists page appears.

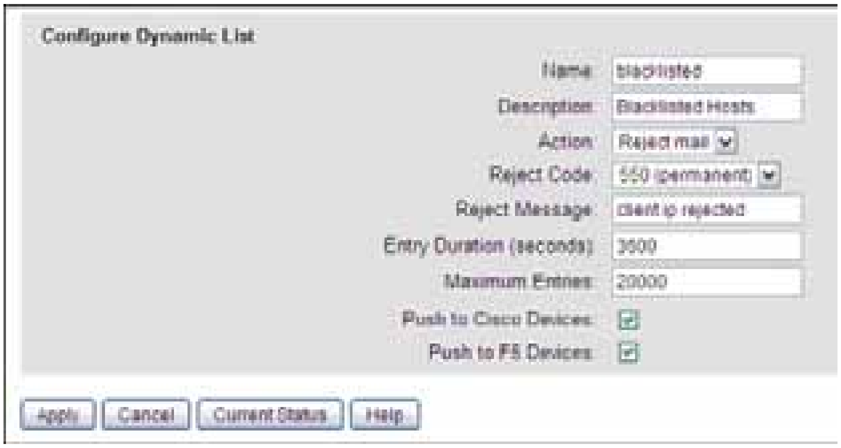


Select	Name	Description	Action	Reject Code	Duration (s)	Max. # Entries	F5	Cisco	
□	blacklisted	Blacklisted Hosts	reject	550	3600	20000			Status
□	harvesters	Directory Harvesters	reject	550	3600	20000			Status
□	infected	Viruses received	reject	550	3600	20000			Status
□	spammers	Spammers	reject	550	3600	20000			Status
□	tarpit	Tar Pit	log	450	3600	1			Status

   There are five predefined data groups:

   - **blacklisted** – Addresses that are blocked.
   - **harvesters** – Addresses known to be involved in email address directory harvesting.
   - **infected** – Addresses known to send virus-infected messages.
   - **spammers** – Addresses known to send large amounts of spam.
   - **tarpit** – Group used to temporarily reject connections to slow down incoming connections from an address.

2. Select a group to edit its properties, or click the **Add** button to add a new group.



Configure Dynamic List

Name: blacklisted

Description: Blacklisted Hosts

Action: Reject mail

Reject Code: 550 (permanent)

Reject Message: client ip rejected

Entry Duration (seconds): 3600

Maximum Entries: 20000

Push to Cisco Devices: ☑

Push to F5 Devices: ☑

- **Name** – Type a descriptive name for this list. If you push data to an F5 or Cisco device, this list name must match the group name configured on the device.
- **Description** – Type a description of this list.
- **Action** – Action to take if a connecting IP address is listed in this group. Options are **Reject Mail** or **Just Log**.
- **Reject Code** – If the selected action is **Reject Mail**, reply to the connection request with this reject code. Select “450” (temporary) or “550” (permanent).
- **Reject Message** – Type the reject reason provided to the client. This message is sent only if the action is set to **Reject Mail**.
- **Entry Duration** – Type the duration (in seconds) for an IP address to remain in this list after it has been placed into this group by a connection rule. This duration period only applies to the groups on the WatchGuard XCS and is not pushed to an F5 or Cisco device.
- **Maximum Entries** – Type the maximum entries allows simultaneously in the list. You can enter a value from 0 to 100000. Set to 0 for unlimited.
- **Push to Cisco Devices** – Push data to all configured Cisco devices. The list name must be identical to the group name defined on the Cisco device. You can only assign one data group to push information to a Cisco device.
- **Push to F5 Devices** – Push data to all configured F5 devices. The Group name must be identical to the group name defined on the F5 device.

3. Click **Apply**.

F5 Devices

You can push Threat Prevention information to an existing F5 device. You can then configure the F5 device to rate limit, throttle, or block a given IP address.

The data groups defined with the Threat Prevention feature are used to populate data groups on the F5 with the same name. For example, IP addresses already defined into a *spammers* group are pushed to the same group name on the F5 device. This allow the F5 to manage the response to these addresses. When an item is removed from a Threat Prevention data group, it is automatically removed from the F5 data group.

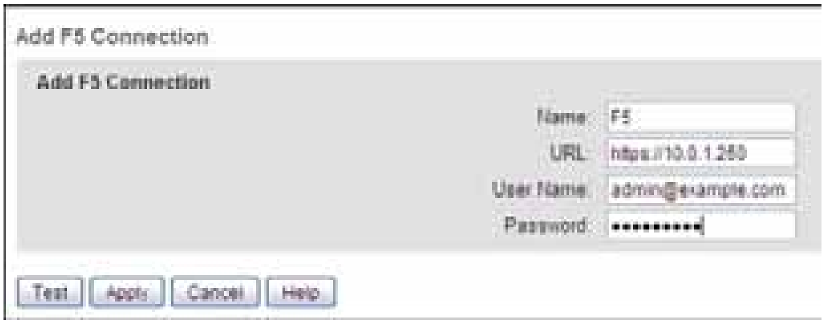
Note that the duration period of the IP address only applies to the data groups on the WatchGuard XCS. The device constantly pushes updated list information to the F5 every 30 seconds to make sure the lists are current and accurate. Any expired IP addresses are removed and new addresses since the last update are added to the F5 device’s list. The data group is also fully synchronized every hour with the F5 device.

You must configure iRules on the F5 device to act on the data groups as appropriate. The Threat Prevention feature does not automatically create iRules on the F5 device.

> ***Note*** *The F5 device must be version 9.0.5 or greater.*

To configure an F5 device:

1. Select **Security > Anti-Spam > Threat Prevention > F5 Devices**.
2. Click **Add**.
   The Add F5 Connection page appears.



Add F5 Connection

Add F5 Connection

Name: F5
URL: https://10.0.1.250
User Name: admin@example.com
Password: ••••••••••

- **Name** – Type a descriptive name to refer to this specific F5 device.
- **URL** – Type the full URL for the F5 device. For example, `https://192.168.1.100`.
- **User Name** – Type a valid user name to log in to the F5 device.
- **Password** – Type a password for the user name.

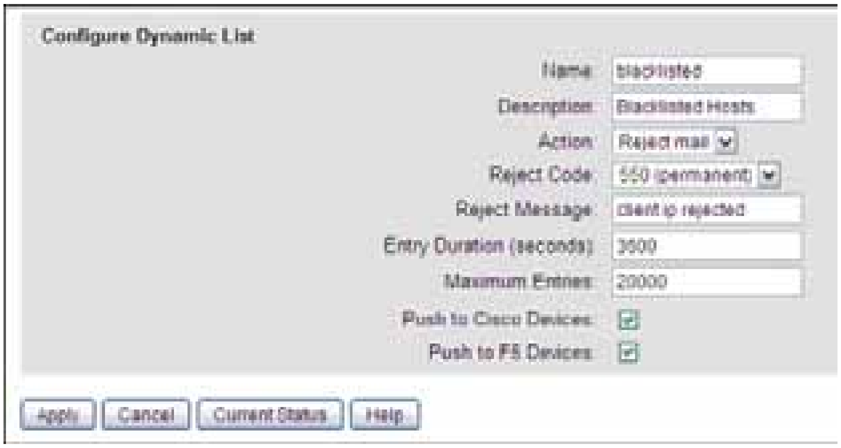
3. To test your connection and login parameters on the F5 device, click **Test**.
4. Click **Apply**.

Enable Data Transfer to an F5 Device

You can push items from the Threat Prevention data groups to the F5 data groups of the same name on one or more F5 devices.

To push data to the F5 device:

1. Select **Security > Anti-Spam > Threat Prevention > Data Groups**.
2. For each data group, make sure you select the **Push to F5 Devices** check box.



Configure Dynamic List

Name:	blacklisted
Description:	Blacklisted Hosts
Action:	Reject mail
Reject Code:	550 (permanent)
Reject Message:	client ip rejected
Entry Duration (seconds):	3600
Maximum Entries:	20000
Push to Cisco Devices:	☑
Push to F5 Devices:	☑

3. Click **Apply**.

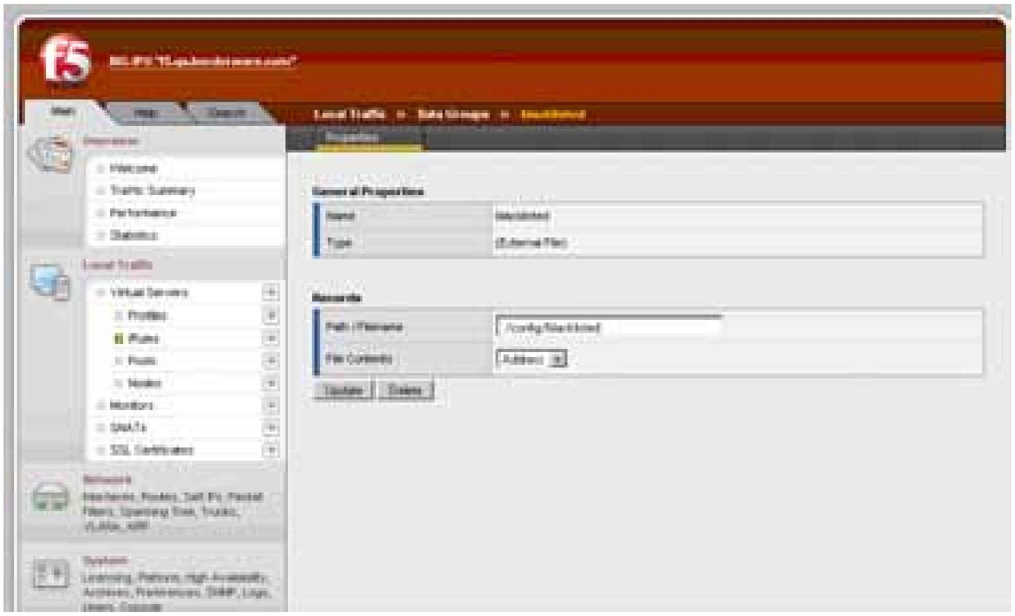
Configure F5 Data Groups

You must manually create the data group names defined on the WatchGuard XCS on the F5 devices. These groups are not automatically created with the Threat Prevention feature.

> **Note** *On the F5 device, you must create the groups as "external file" address data groups, not address groups. External file address groups are updated frequently with many IP addresses without affecting F5 performance.*

To create groups on the F5 device:

1. Log in to the F5 administration interface.
2. Select **Local Traffic > iRules**.
3. Click the **Data Group** list tab.
4. Click **Create**.
5. Type the same group name as the data group defined in the Threat Prevention feature.
6. Select **External file** (not Address).
   A subset of options appear.
7. Type the group name and select **Address** in the **File Contents** list.


BIG-IP® "TLsp.bordeware.com"
Main
Help
Search
Overview
Welcome
Traffic Summary
Performance
Statistics
Local Traffic
Virtual Servers
Profiles
iRules
Pools
Nodes
Monitors
SNATs
SSL Certificates
Network
Interfaces, Routes, Self IPs, Packet Filters, Spanning Tree, Trunks, VLANs, ARP
System
Licensing, Platform, High Availability, Archives, Preferences, SNMP, Logs, Users, Console
Properties
Update
Delete

Local Traffic » Data Groups » blacklisted

General Properties

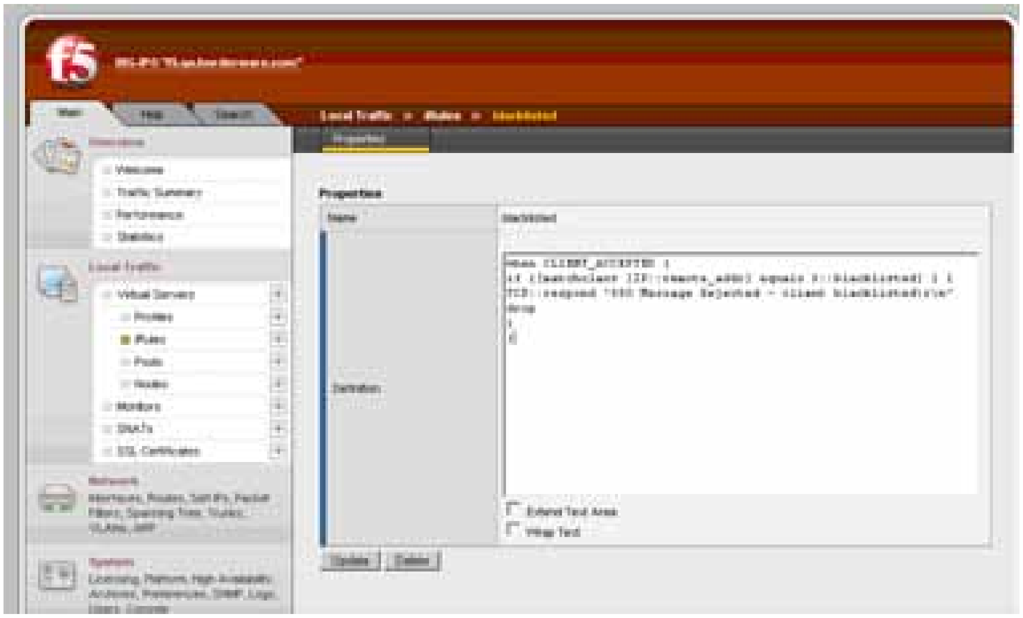
Name	blacklisted
Type	(External File)

Records

Path / Filename	/config/blacklisted
File Contents	Address

8. Click **Finished**.
9. Repeat the steps for each data group.

   You must perform this procedure on each F5 device.
10. Create an iRule for the data group.


BIG-IP® "TLsp.bordeware.com"
Main
Help
Search
Overview
Welcome
Traffic Summary
Performance
Statistics
Local Traffic
Virtual Servers
Profiles
iRules
Pools
Nodes
Monitors
SNATs
SSL Certificates
Network
Interfaces, Routes, Self IPs, Packet Filters, Spanning Tree, Trunks, VLANs, ARP
System
Licensing, Platform, High Availability, Archives, Preferences, SNMP, Logs, Users, Console
Properties
Update
Delete

Local Traffic » iRules » blacklisted

Properties

Name: blacklisted

Definition:

```
when CLIENT_ACCEPTED {
if {[matchclass [IP::remote_addr] equals $::blacklisted] } {
TCP::respond "550 Message Rejected - client blacklisted\r\n"
drop
}
}
```

□ Extend Text Area
□ Wrap Text

This is a typical iRule for the default set of data groups provided with Threat Prevention:

```
when CLIENT_ACCEPTED {
   if {[matchclass [IP::remote_addr] equals $::harvesters] }
{        TCP::respond "550 Message Rejected - Too many unknown recipients\r\n"
      drop    }
```

```
    if {[matchclass [IP::remote_addr] equals $::spammers] }
{      TCP::respond "550 Message Rejected - Too much spam\r\n"      drop   }
    if {[matchclass [IP::remote_addr] equals $::blacklisted] }
{       TCP::respond "550 Message Rejected - client blacklisted\r\n"
drop   }
   if {[matchclass [IP::remote_addr] equals $::infected] }
{    TCP::respond "550 Message Rejected - Infected\r\n"    drop
}  if {[matchclass [IP::remote_addr] equals $::tarpit] } {    pool slow_rateclass
 }}
```

11. Create any rate shaping classes, virtual hosts, and pools, as necessary for normal configuration of an MTA.

    In the previous example, a pool called “slow_rateclass” is required that is configured with rate shaping to allow a limited rate of traffic.

12. To verify you have configured the F5 device correctly in the Threat Prevention feature, on the WatchGuard XCS, select **Security > Anti-Spam > Threat Prevention > F5 Devices**, and click **Test**.

    The WatchGuard XCS attempts to list the contents of the F5 data group.

    If successful, the list of IP addresses that have been pushed to the F5 device appear. The test feature does not interrupt mail delivery or communications with the F5.

    > ***Note*** *In F5 version 9.0.5, you cannot view the contents of external file data groups from the F5 web interface. Use the Test button in the Threat Prevention menu to view the contents of external file data groups.*

WatchGuard XCS and F5 Integration Notes

Note these considerations when you integrate the WatchGuard XCS and an F5 device:

- The Threat Prevention feature updates continuously but also synchronizes with each F5 Data Group once an hour to make sure there are no discrepancies.
- If the F5 device does not contain a data group, Threat Prevention attempts to synchronize with it once every second. It reports the warning once every 30 seconds in the mail logs for this condition.
- If there is a loss of communications between the WatchGuard XCS and the F5 device, the Threat Prevention feature retries the connection to the F5 up to ten times.
- When you use F5 integration with a cluster, only the Primary device’s data groups are pushed to the F5 device.

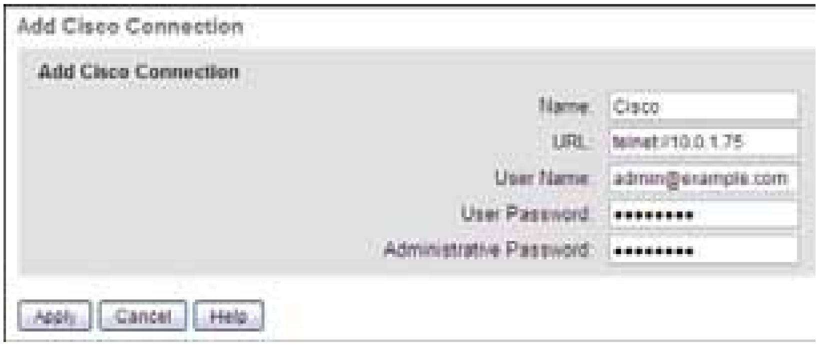
Cisco Devices

You can push Threat Prevention information to an existing Cisco device. The WatchGuard XCS can update the Cisco device with information from a single data group. To configure the Cisco device to block a given IP address, add the IP address to an appropriate ACL (Access Control List). When an item is removed from the Threat Prevention list, it is automatically removed from the Cisco IP access list.

> ***Note*** *The system utilizes the IP named access control list feature to forward information to the Cisco device. Cisco IOS version 11.2 or later is required for WatchGuard XCS and Cisco integration.*

To configure a Cisco device:

1. Select **Security > Anti-Spam > Threat Prevention > Cisco Devices**.
2. Click **Add**.
   The Add Cisco Connection page appears.



Add Cisco Connection

Add Cisco Connection

Name: Cisco
URL: telnet://10.0.1.75
User Name: admin@example.com
User Password: ••••••••
Administrative Password: ••••••••

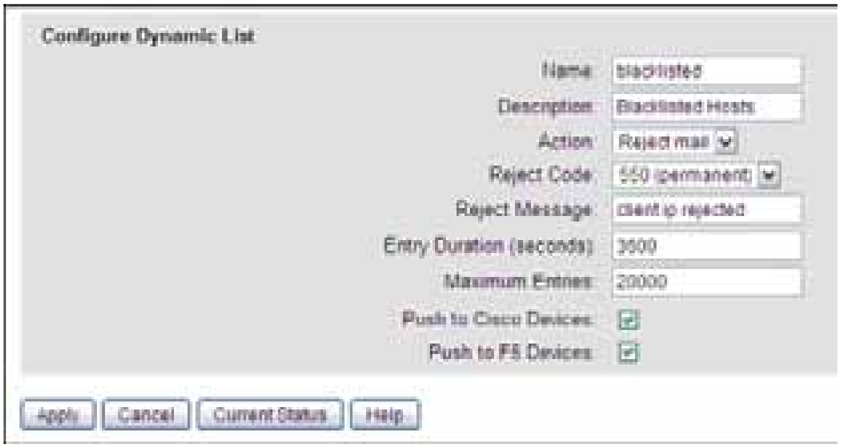
- **Name** – Type a descriptive name to refer to this specific Cisco device.
- **URL** – Type the full telnet URL for the Cisco device. For example, `telnet://192.168.1.175`.
- **User Name** – Type a valid user name to log in to the Cisco device.
- **User Password** – Type a corresponding password for the user name.
- **Administrative Password** – Type the administrative (enable) password for this Cisco device.

3. Click **Apply**.

Enable Data Transfer to a Cisco Device

The Threat Prevention feature pushes items from a defined data group to an IP access list on a Cisco device. To push data to the Cisco device.

1. Select **Security > Anti-Spam > Threat Prevention > Data Groups**.



Configure Dynamic List

Name: blacklisted
Description: Blacklisted Hosts
Action: Reject mail
Reject Code: 550 (permanent)
Reject Message: client ip rejected
Entry Duration (seconds): 3600
Maximum Entries: 20000
Push to Cisco Devices: ☑
Push to F5 Devices: ☑

2. For the data group you want to push, select the **Push to Cisco Devices** check box.

The Cisco device can only accept one data group. We recommend that you use the **blacklisted** list to block clients on the Cisco device.

The duration period of the IP addresses only apply to the data groups on the WatchGuard XCS. The WatchGuard XCS constantly pushes updated list information to the Cisco device every 30 seconds to make sure the lists are current and accurate.

Any expired IP addresses are removed and new addresses since the last update are added to the Cisco device's list. The data group is also fully synchronized with the Cisco device every hour.

For IOS version 12.1 and later, Threat Prevention lists are automatically created on the Cisco device when group information is pushed, however, the IP access group must still be assigned to a specific interface.

Warning *Make sure that the Maximum Entries value is customized to the capabilities of your Cisco device. Large values can overrun a Cisco device that can only handle a certain amount of access list entries.*

3. Click **Apply**.

Cisco Device Configuration

To configure the Cisco device:

1. Log in to the Cisco device with the "enable" privilege.
2. Change to configure mode:

```
# configure terminal
```

3. Change to interface mode (where x and y are the Ethernet interface):

```
# interface FastEthernet x/y
```

4. Attach the IP access group to the WatchGuard XCS data group:

```
# ip access-group <access_list_name> in
```

5. Exit from the config-if mode:

```
# exit
```

6. Perform the same steps for each Cisco interface as required.

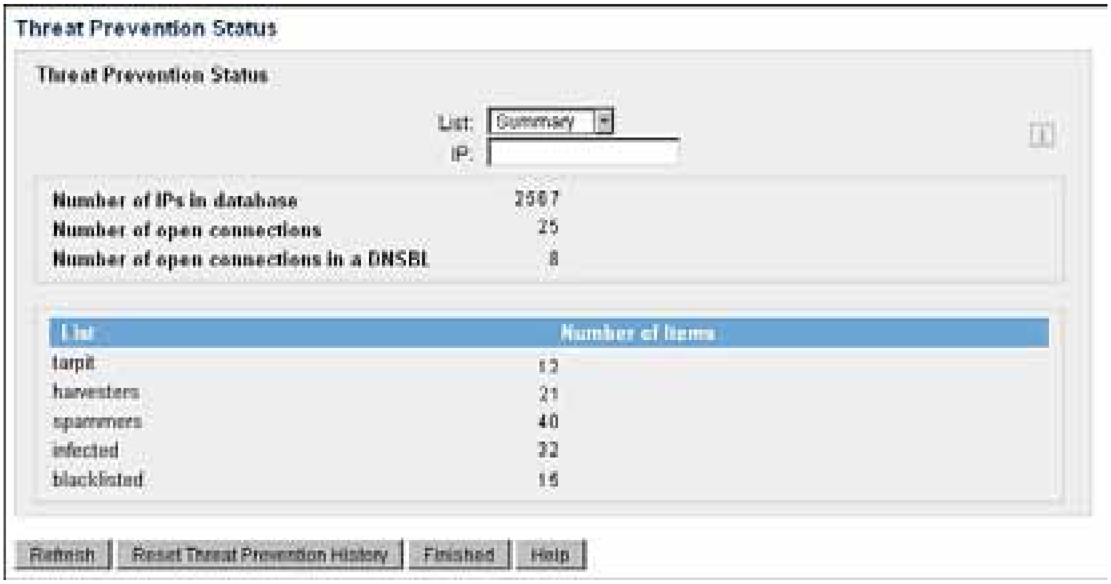
Threat Prevention Status

The Threat Prevention Status page displays the current state of the threat prevention feature and provides information on the current number of items in each specified list, for example, the number of addresses listed as *spammers*.

To view the current threat status, select **Activity > Status > Threat Prevention**.

A summary of the entire threat prevention database appears. This information includes:

- The number of IP addresses in the Threat Prevention database
- The number of open connections and open connections in a DNSBL
- The number of items in each defined data group, for example, *tarpit*, *harvesters*, *spammers*, *infected*, and *blacklisted*.



Threat Prevention Status

Threat Prevention Status

List: Summary

IP:

Number of IPs in database	2567
Number of open connections	25
Number of open connections in a DNSBL	8

List	Number of Items
tarpit	12
harvesters	21
spammers	40
infected	22
blacklisted	15

To search for the state of a specific IP address, type the address in the **IP** text box. A new table appears for that specific IP address, and displays statistics on the number of messages from that IP address during a specific time period and the types of messages received.

To reset the status data and clear the Threat Prevention database, click **Reset Threat Prevention History**.

17 Clustering

About Clustering

Clustering provides a highly scalable, redundant messaging security infrastructure that enables two or more WatchGuard XCS devices to act as a single logical unit for processing messages for redundancy and high availability benefits.

There is no theoretical limit to the size of the cluster, and you can add devices to the cluster to increase processing and high-availability capabilities. When you use Clustering, message traffic flow is never interrupted because of individual device failures.

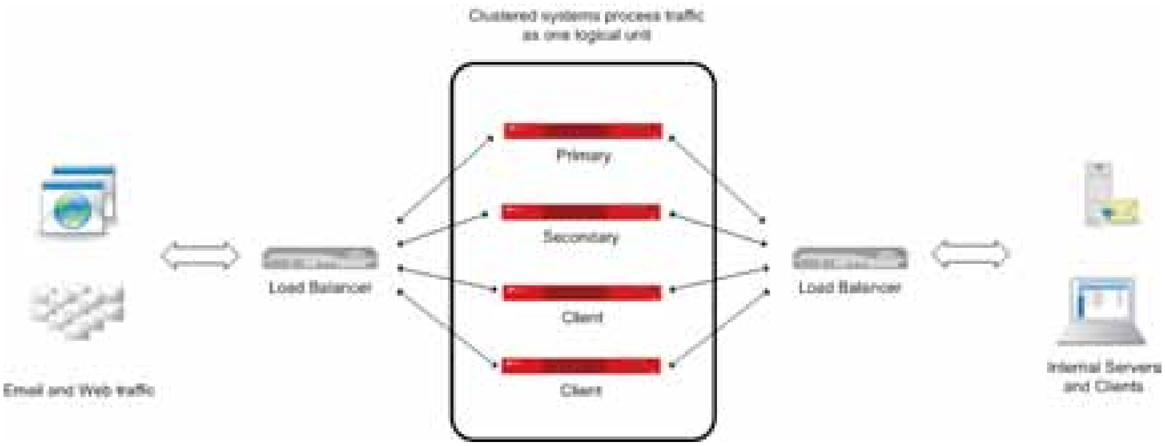
You can manage a cluster from any single device in the cluster, and all devices in the cluster can process messages. Any configuration changes, for example, Anti-Spam and Policies, are propagated to all cluster devices.

Cluster Architecture

The WatchGuard XCS devices participating in the cluster communicate together through a network interface connected to a separate network called the *cluster network*. The cluster network is a dedicated, physically secure subnet, and the devices communicate clustering information with each other through this network. You can add or remove devices from the cluster network without interruption to message processing.

> ***Note*** *Cluster members must be connected together on the same network.*

The WatchGuard XCS clustering architecture is illustrated in this diagram.


Clustered systems process traffic as one logical unit
Primary
Secondary
Client
Client
Load Balancer
Load Balancer
Email and Web traffic
Internal Servers and Clients

The WatchGuard XCS operates in one of four different modes in a cluster:

- **Primary** – This device is the primary master system for the cluster. All configuration is performed on this device. Other devices in the cluster pull configuration changes from the Primary automatically when you apply a new configuration.
- **Secondary** – A device running in Secondary mode operates the same way as a Client cluster device except that it retains a copy of the master database replicated from the Primary. If the Primary cluster device fails, the Secondary can be promoted to Primary status.
- **Client** – A device that runs in Client mode pulls its configuration from an existing Primary. After the initial setup, no configuration is required on the Client. You can promote a Client to a Secondary. Unlike a Primary or Secondary, a Client does not contain a copy of the full configuration database.
- **Standalone** – The device initially installs in Standalone mode. In this mode, the device still processes mail, but does not participate as part of the cluster and does not pull configuration updates. This mode is primarily used to remove a cluster device for offline maintenance or software updates.

Load Balancing

Although the cluster is treated as one logical system for processing messages, network traffic is processed independently by each cluster device and requires the use of a load balancing system to distribute mail flow between the devices in the cluster.

Email load balancing with DNS

You can use a DNS round-robin technique to distribute incoming SMTP mail connections to the devices in the cluster. For example, add these entries to your DNS MX records to distribute mail to two different WatchGuard XCS devices.

```
example.com IN MX 10 mail1.example.com

example.com IN MX 10 mail2.example.com
```

Assign different priority values to give priority to specific devices. For example:

```
example.com IN MX 5 mail1.example.com

example.com IN MX 10 mail2.example.com
```

> ***Note*** *Load balancing for specific types of network traffic (for example, HTTP) is not possible with DNS round-robin techniques.*

Traffic Load Balancing with a Load Balancer Device

You can also use a hardware load balancing device to send messages to different WatchGuard XCS devices in a cluster. If one of the devices fails, the load balancer distributes the load between the remaining devices. You can configure the load balancer to distribute the mail stream connections intelligently across all devices in the cluster based on device load and availability.

External load balancing devices are mandatory if you need to route specific traffic (for example, SMTP and HTTP) through specific hosts in the cluster. For example, SMTP mail can be processed by two cluster devices, while HTTP is handled by another two different devices. You can configure the load balancer to route protocol-specific traffic as required.

Configure Clustering

These are the steps to install and configure a cluster:

1. **Hardware and Licensing** – Make sure that all devices use the same hardware and run the identical, licensed versions of software. This includes any software updates.
2. **Cluster Network Configuration** – Configure a network interface on each device for clustering.
3. **Select a Cluster Mode** – For each device in the cluster, you must choose a mode for the device to run in (Primary, Secondary, Client, Standalone). The first device must be the Primary, the second Secondary, and other devices can be configured as a Secondary or Client.

Hardware and Licenses

All cluster devices must be the same level of hardware, be properly licensed, and run the identical version of software (this includes patches and updates). Any feature key discrepancies appear in the Cluster Activity page.

Cluster devices should be new installations with no changes to the default configuration. When a device is connected to the cluster, it receives its configuration from the Primary.

Cluster Network Configuration

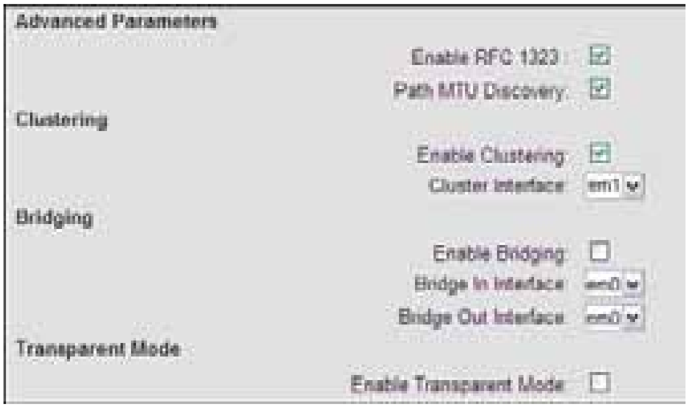
To configure the network settings for two devices in a cluster:

1. Connect an unused network interface from each device in the cluster to a common network switch, or connect each interface with a crossover network cable. This forms the cluster network, a control network where clustering information is passed back and forth between the devices that form the cluster.

   For security reasons, this network must be isolated and not be connected to the main network. For a cluster of two devices, you can connect a crossover network cable between the selected interfaces to provide a secure connection without the need for a network switch.

2. On each device, select **Configuration > Network > Interfaces**.
3. In the **Clustering** section, select the **Enable Clustering** check box.
4. Select the network interface connected to the cluster network.

   This interface must not be configured with an IP address. The interface is automatically configured for exclusive use on the cluster network.



Advanced Parameters

Enable RFC 1323: ☑
Path MTU Discovery: ☑

Clustering

Enable Clustering: ☑
Cluster Interface: em1

Bridging

Enable Bridging: □
Bridge In Interface: em0
Bridge Out Interface: em0

Transparent Mode

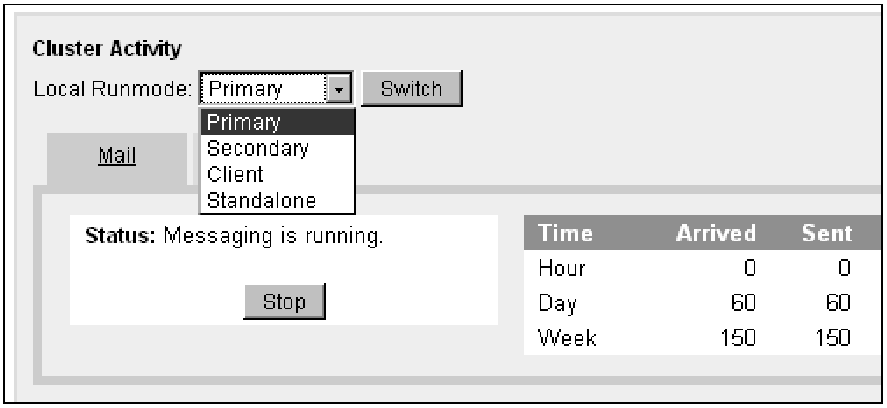
Enable Transparent Mode: □

5. Make sure that an NTP time server is configured on each device, and add additional NTP servers for redundancy.
   You cannot enable clustering until you configure an NTP server. The time server synchronizes all cluster devices from a common time source.
6. Click **Apply**.
   You must restart the system.

Select a Cluster Mode

When the WatchGuard XCS restarts, select a cluster mode for this device. Initially, the device starts in Standalone mode. The first device set up in the cluster must be designated as the Primary system.

1. Select **Activity > Status > Cluster Activity**.



Cluster Activity

Local Runmode: Primary

Status: Messaging is running.

Time	Arrived	Sent
Hour	0	0
Day	60	60
Week	150	150

2. From the **Local Runmode** drop-down, select **Primary**.
3. Click **Switch**.

For your other cluster devices, configure at least one device as the Secondary. You can configure the other devices as a Secondary or Client. When you add devices to a cluster, the configuration of the Primary is replicated automatically to the new cluster device.

When you have configured all of your clustered devices, the Cluster Activity page displays the mode and status of the other members of the cluster.

Cluster Management

All cluster configuration is performed from the Primary. When a device is added to the cluster for the first time, the configuration of the Primary is replicated to the new cluster member, except these items:

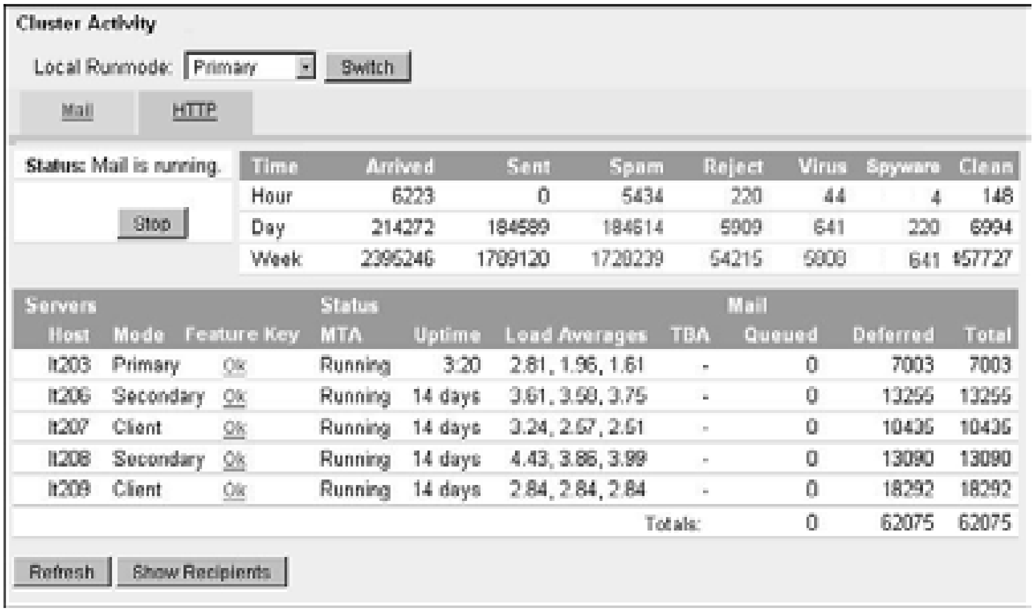
- Unique networking settings, for example, the host name and IP address, and network interface specific settings
- Performance settings and SSL Certificates
- Local users
- Secure WebMail configuration (in a clustered environment, the Secure WebMail proxy can only be enabled on the Primary in the cluster)
- Reports and logs
- Token analysis spam training databases
- Web Proxy PAC files
- Vacation notifications
- User Spam Quarantine

Any changes to the configuration of the Primary results in a broadcast notifying the other members of the cluster that a change has been made. The other devices in the cluster then pull the updated configuration from the Primary.

Cluster Activity

The main *Cluster Activity* page displays processing statistics for the entire cluster.

Select **Activity > Status > Local Activity** to see the statistics only for this specific device.



Cluster Activity

Local Runmode: Primary

Status: Mail is running.

Time	Arrived	Sent	Spam	Reject	Virus	Spyware	Clean
Hour	6223	0	5434	220	44	4	148
Day	214272	184589	184614	5909	641	220	6994
Week	2395246	1709120	1720239	54215	5000	641	157727

Servers			Status				Mail		
Host	Mode	Feature Key	MTA	Uptime	Load Averages	TBA	Queued	Deferred	Total
lt203	Primary	Ok	Running	3:20	2.81, 1.96, 1.61	-	0	7003	7003
lt206	Secondary	Ok	Running	14 days	3.61, 3.59, 3.75	-	0	13256	13256
lt207	Client	Ok	Running	14 days	3.24, 2.67, 2.61	-	0	10436	10436
lt208	Secondary	Ok	Running	14 days	4.43, 3.86, 3.99	-	0	13090	13090
lt209	Client	Ok	Running	14 days	2.84, 2.84, 2.84	-	0	18292	18292
						Totals:	0	62075	62075

Mail Statistics

The queue statistics columns for email are:

- **Arrived** – The total number of messages processed by the cluster (messages accepted). These include messages that are spam, viruses, and filtered because of content.
- **Sent** – The total number of messages sent by the cluster. This includes mailer daemon mail, quarantine notifications, mail delivery delay notifications, local mail, alarms, and reports. If a message has multiple recipients, each delivered recipient is added to the total.
- **Spam** – The total number of messages classified as spam by Intercept for the cluster. This includes Certainly Spam, Probably Spam, Maybe Spam, and rejected spam messages. This category is based on the Spam logging configuration in **Configuration > Miscellaneous > Reports**. The spam action of **Just Log** is counted in the total if you enable it in the spam logging configuration.
- **Reject** – The total number of messages rejected because of these features:
  - Reject on unknown sender domain
  - Reject on missing sender MX
  - Reject on non FQDN sender
  - Reject on unauth pipelining
  - Reject on Unknown Recipient
  - Relay Access Denied
  - Threat Prevention Reject
  - Reputation Enabled Defense Reject (Reputation, Infected, Dial-up)
  - DNS Block List Reject
  - Specific Access Pattern Reject
  - Pattern Filter reject
  - Anti-Spam Reject (is also included in Anti-Spam statistics column)
  - Anti-Virus Reject (is also included in Anti-Virus statistics column)
  - Attachment Control Reject
  - Objectionable Content Filter Reject
  - Content Scanning Reject
- **Virus** – The total number of virus-infected messages. This includes rejected messages.
- **Spyware** – The total number of spyware-infected messages. This includes rejected spyware messages.
- **Clean** – The total number of messages accepted for delivery inbound and outbound by the WatchGuard XCS that passed all security and spam/content filters. This includes messages detected by these features that have an action of **Just Log**.

HTTP Statistics

The statistics columns for the HTTP Proxy are:

- **HTTP Requests** – The total number of incoming and outgoing HTTP requests.
- **Reject** – The total number of web requests rejected because of the threat and content control scanners.
- **Virus** – The total number of web requests blocked because the web site contained a virus.
- **Spyware** – The total number of web requests blocked because the web site contained spyware.

Servers

The statistics and information provided in the **Servers** section of the Cluster Activity page are:

- **Host** – Indicates the host name of the cluster device.
- **Mode** – Indicates which cluster mode the specific host is running in, for example, Primary, Secondary, or Client.
- **Feature Key** – All cluster devices must have the same licensed features. This column indicates if the feature key is "OK" for this cluster device, or a "Mismatch" appears if the feature key on this host does not match the other devices in the cluster.
- **Status** – Indicates if the cluster device is currently "Running" and processing messages or "Stopped".
- **Uptime** – Indicates how long this cluster device has been running since its last restart.
- **Load Averages** – Indicates CPU load for this cluster device over 1 minute, 5 minutes, and 15 minutes.
- **Queued** – Indicates how many messages are currently in the Mail Queue waiting to be delivered. You can view and manage these messages in **Activity > Queue/Quarantine > Mail Queue**.
- **Deferred** – Indicates the number of messages that have their delivery deferred because the destination mail server is unavailable. The WatchGuard XCS attempts to deliver these messages at a later time.
- **Total** – The total of all messages that are queued for delivery or deferred on this cluster device.

Stop and Start Messaging Queues

If you click the **Stop** or **Start** messaging button on a cluster device, this action applies on all devices in the cluster.

To modify an individual cluster device's messaging status, change the run mode to Standalone, and then click the **Stop** or **Start** messaging button as required. The full main menu is only available on the Primary system. Secondary and Client devices only show a subset of options because most of the configuration is replicated from the Primary.

Change Cluster Run Mode

If a Primary device fails, you can log in to the Secondary and change its mode to Primary. A Client must be first promoted to a Secondary before it can be promoted to a Primary. This is because a Client, unlike a Secondary, does not contain a copy of the Primary's database.

To change the mode of a cluster device:

1. Log in to the device you want to modify.
2. On the Cluster Activity page, from the **Local Runmode** drop-down box, select a new mode.
3. Click **Switch**.

Cluster System Maintenance

Use the Standalone cluster mode to perform maintenance on a device, for example, to update a feature key, make hardware modifications, perform software updates, and troubleshoot issues. In Standalone mode, the device still processes messages, but does not receive configuration updates from the Primary. This prevents configuration misalignment between devices with different software versions or licensed features.

> ***Note*** *It is critical that you set a cluster system to Standalone mode when you perform any feature key or software updates.*

When you have finished the system maintenance and restarted the device, you can set the mode of the device back to its original cluster state. The device returns to the cluster and continues to process mail. Configuration replication from the Primary resumes when you have rejoined the device to the cluster.

Unlike a Primary or Secondary, a Client does not contain a copy of the configuration database. When you switch between Client and Standalone modes, this can result in the user interface configuration of the Standalone not reflecting its actual configuration as a Client in the cluster. To make sure a Client has the latest configuration changes, set its mode to Secondary and wait 15 minutes before you set the mode to Standalone.

Perform a System Update on a Cluster Device

To perform a system update, for example, a feature key or software update, in a cluster consisting of a Primary, a Secondary, and a Client:

1. On all devices in the cluster, change the cluster run mode to **Standalone** mode.
2. Perform the update on the **Primary**, and then restart the system.
3. Change the run mode of the **Primary** system from **Standalone** back to **Primary** mode.
4. Perform the update on the **Secondary**, and then restart the system.
5. Change the run mode of the **Secondary** system from **Standalone** back to **Secondary** mode.
6. Perform the update on any **Client** systems, and then restart the system.
7. Change the run mode of the **Client** systems from **Standalone** back to **Client** mode..

This procedure makes sure that while the devices are updated, there are no configuration changes to the cluster.

Cluster Reports and Message History

In clustered environments, reports generate information aggregated for the entire cluster. System and Resource reports display information for each host in the cluster. You can also search the message database on a single device or on the entire cluster. The history and status of any message is instantly retrieved regardless of which device processed the message.

Cluster Device Failures

If a device in a cluster fails, all traffic is still processed by the remaining cluster devices. If you use load balancing devices or DNS round-robin techniques, traffic is routed to the other devices in the cluster. If a Primary device fails, all traffic is still processed by the remaining devices, but you cannot make configuration changes to the cluster. You must promote a Secondary device to Primary mode to allow further configuration changes to the cluster.

Backup and Restore in a Cluster

In a cluster, all Secondary and Client cluster devices pull their configuration directly from the Primary, and it is critical that you back up the Primary configuration on a regular basis to preserve your cluster configuration. Backup Secondary and Client devices if you want to retain their mail queues, quarantined messages, and any reporting data.

Recover a Primary Cluster System

In the event a Primary system fails, you must promote an existing Secondary system to Primary. When the issue with your original Primary is resolved, it should be restored (this includes any mail queues, quarantined messages, and reporting data) and reinserted into the cluster as a Secondary system. Operating as the Secondary, this device pulls an updated cluster configuration from the Primary. If required, this device can be promoted back to its original Primary mode.

Recover a Secondary and Client Cluster System

If a cluster member that is a Secondary or Client fails and cannot be recovered, it must be reinstalled and inserted back into the cluster in its original cluster mode (Secondary or Client) where it then pulls its configuration information from the Primary. Configuration items specific to this cluster device, for example, network settings, SSL certificates, performance settings, and SNMP configuration, must be manually reconfigured. If you have backed up mail queues, quarantined messages, and reporting data for these devices, you can restore them individually without restoring the system configuration from backup.

Threat Prevention and Clustering

When you use Threat Prevention features in a clustered environment, you only need to configure Threat Prevention on the Primary device of the cluster.

> ***Note*** *Threat Prevention decisions are based on per device statistics, and not on statistics for the entire cluster.*

The Primary is also the only point of contact between the cluster and any configured load balancing devices. If you demote a Primary, and promote a Secondary to be Primary, the cluster switches control and resynchronizes to the load balancing device. Threat Prevention still runs independently on each device in the cluster, but only the Primary pushes data to the external devices. See *About Threat Prevention* for more detailed information.

Clustering and Centralized Management

Clusters are used for high availability and load balancing of messages for a single site, and typically include devices with identical configurations. Centralized Management allows you to monitor and manage multiple clusters and independent devices with unique configurations for an entire organization.

Centralized Management is a separate function than clustering. You can use Centralized Management in conjunction with clustering, especially in environments where individual devices and clusters are located in different geographical locations or require a unique configuration.

Centralized Management allows you to treat each cluster as a single Entity within the Federation. You only need to add the Primary device of each cluster to the Centralized Management Federation. If you synchronize a configuration to the Primary of the cluster, the clustering configuration replication process applies the configuration to the other devices (for example, Secondary and Clients) in the cluster. For a Manager system, the Secondary system in the cluster can take over as the Manager system if the Primary is unavailable.

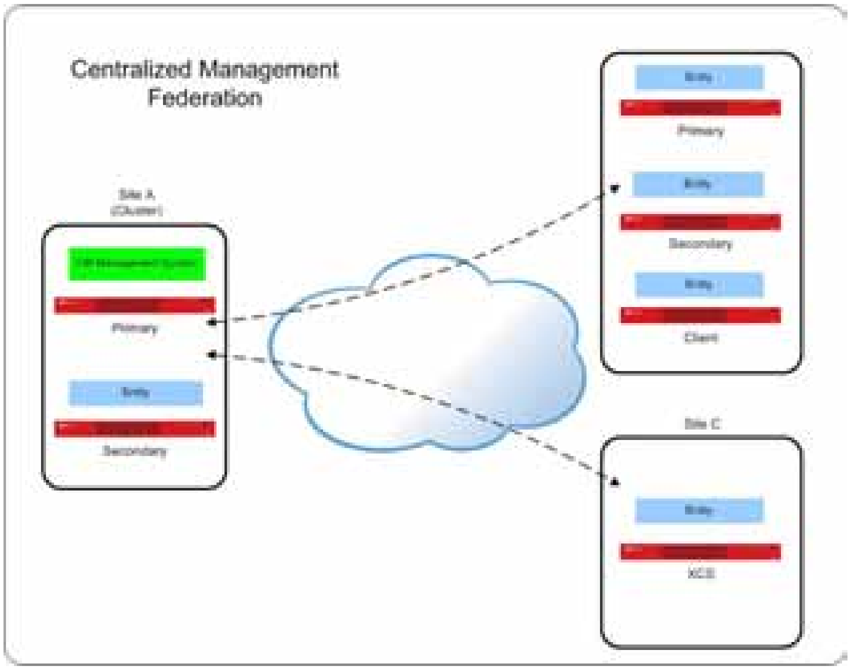
See *About Centralized Management* for more detailed information.

18 Centralized Management

About Centralized Management

Centralized Management allows you to efficiently monitor and manage several WatchGuard XCS devices, running independently or as part of a cluster, from a single management system. In large enterprise networks, there can be several WatchGuard XCS devices operating as clustered or non-clustered systems that are located in geographically distant locations. Each of these devices can have several shared configuration parameters and also require unique configurations for their particular location.

A set of clustered or non-clustered devices that are monitored and managed by Centralized Management are called a *Federation*. Each device within the Federation is called an *Entity*. The Manager system acts as the single point of management and provides the ability to add clustered and non-clustered Entities to the Federation.



All communication between the Manager and Entity systems in a Federation is secure to make sure that communication between devices are not intercepted or decoded by third-parties. Control messages between devices are authenticated to make sire they originate from authorized entities in the Federation.

Centralized Management and Clustering

Centralized Management is a separate function than clustering. You can use Centralized Management in conjunction with clustering, especially in environments where individual devices and clusters are located in different geographical locations or require a unique configuration.

Clusters are used for high availability and load balancing of messages for a single site, and typically include devices with identical configurations. Centralized Management allows you to monitor and manage multiple clusters and independent devices with unique configurations for an entire organization.

Centralized Management allows you to treat each cluster as a single Entity within the Federation. You only need to add the Primary device of each cluster to the Centralized Management Federation. If you synchronize a configuration to the Primary of the cluster, the clustering configuration replication process applies the configuration to the other devices (for example, Secondary and Clients) in the cluster. For a Manager system, the Secondary system in the cluster can take over as the Manager system if the Primary is unavailable.

Centralized Management Features

Centralized Management provides these features and benefits:

- Allows you to group a Manager and Entity devices (this includes clustered and non-clustered devices) into a single Centralized Management Federation.
- Allows you to monitor the activity and status of all Entities in the Federation from the Manager device.
- Allows you to define a global configuration set that you can apply to all Entities in a Federation (this includes independent devices and clusters). Most aspects of the configuration are available for distribution. This includes message delivery settings, policies, policy mappings, and mail routes.
- You can modify the local configuration of Entity devices in the Federation for unique local requirements.
- You can view reports from all Entities in the Federation on the Manager system.
- You can search the Message History of all Entities in the Federation on the Manager system.

Deployment

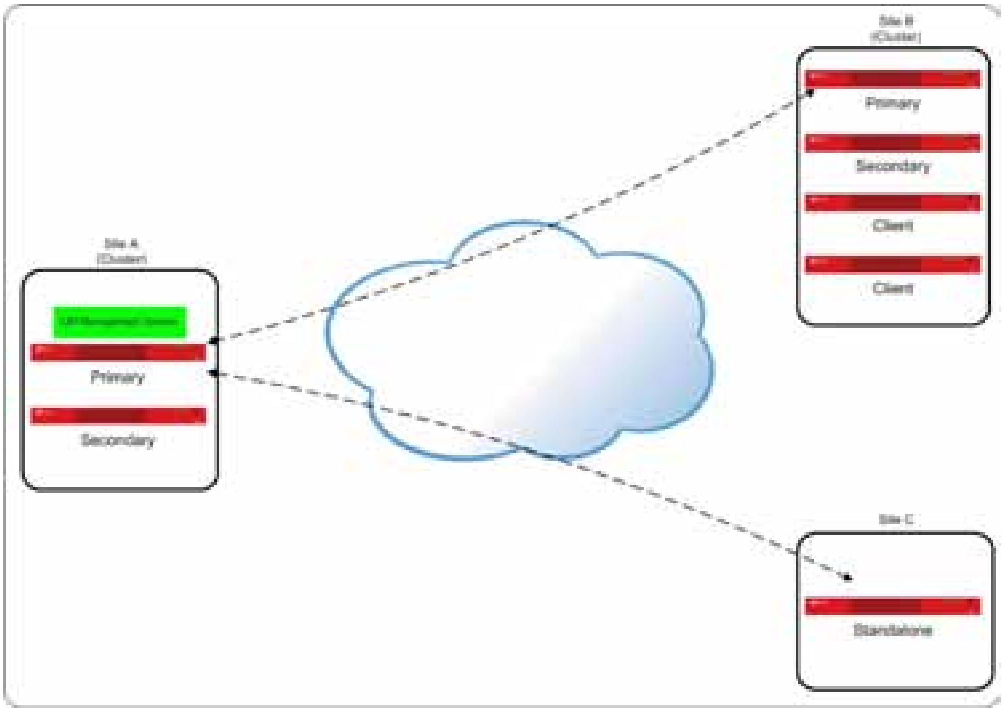
Centralized Management can be deployed on any type of WatchGuard XCS device. This includes clustered and non-clustered systems. The device running as the Manager can still process messages and perform security processing independently or as part of an existing cluster.

Centralized Management in a Cluster

In this deployment, the Centralized Management device is running in a cluster at the main organizational site running on the Primary system. In this configuration, the Secondary cluster system can take over as the Manager system if the Primary is not available.

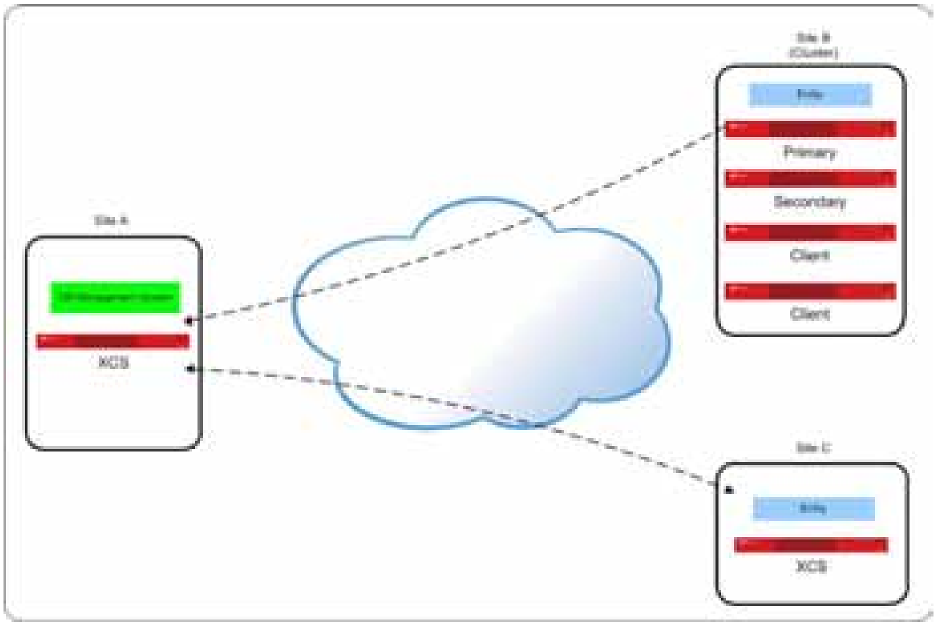
The Manager system can monitor and manage other Entities in the Federation. This includes entire clusters (Site B), or independent non-clustered devices (Site C).

When you add a cluster to a Federation, you only need to add the Primary for that cluster. All configuration items synchronized from a Configuration Set to the Primary are automatically replicated to the Secondary and Client devices as part of the clustering configuration replication process.



Centralized Management on a non-Clustered System

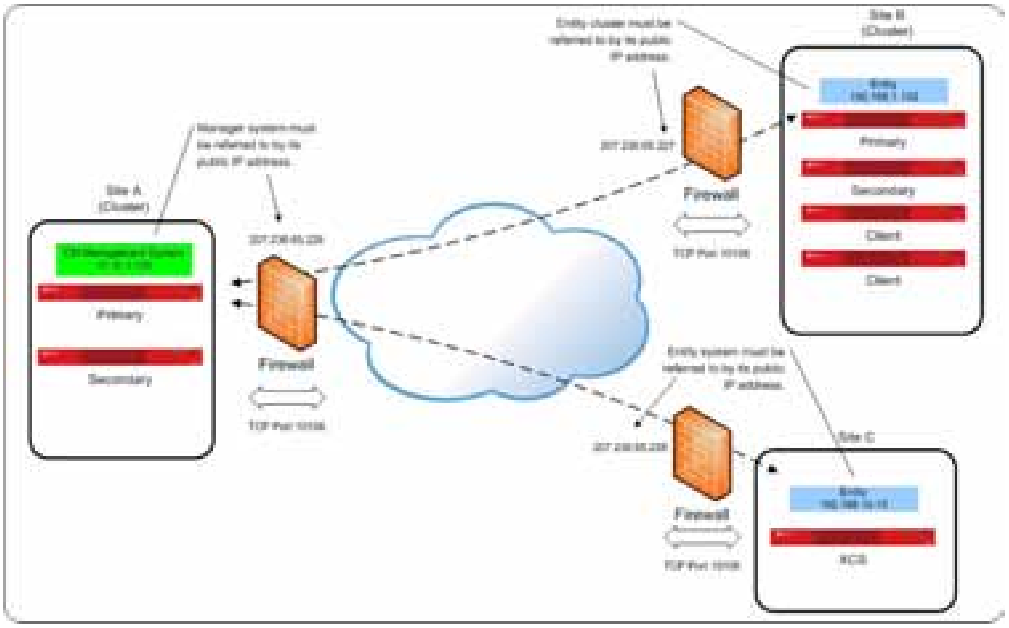
You can also deploy the Manager device on an independent non-clustered system while managing both clustered (Site B), and non-clustered sites (Site C) in other locations.



Networking Ports and Addresses

Centralized Management uses TCP port 10106 to communicate between systems in the Federation. You must open this port inbound and outbound on a network firewall if the devices are located behind the firewall.

If the IP addresses are NAT (Network Address Translation) addresses, you must specify the Entities and Manager with the public address of the firewall. You can do this during the Entity configuration process when you add the Entities to the Manager system.


Entity cluster must be referred to by its public IP address
Site B
(Cluster)
Entity
Primary
Secondary
Client
Client
Firewall
TCP Port 10106
Manager system must be referred to by its public IP address
Site A
(Cluster)
Primary
Secondary
Firewall
TCP Port 10106
Entity system must be referred to by its public IP address
Site C
Entity
XCS
Firewall
TCP Port 10106

Create a Centralized Management Federation

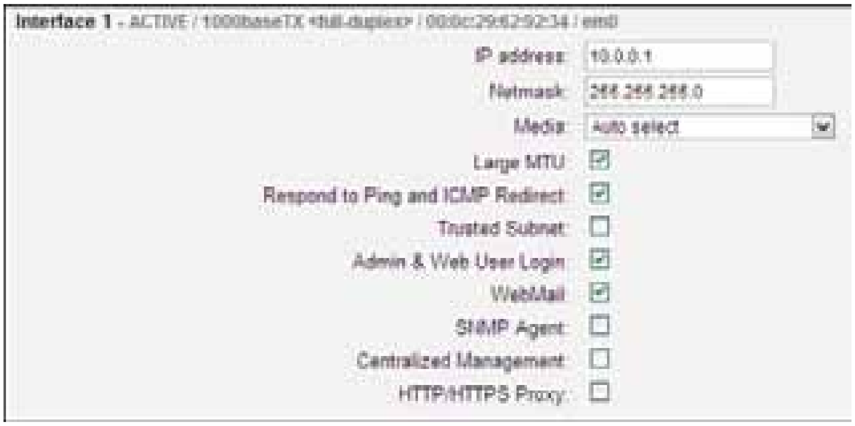
To configure Centralized Management:

- Enable Centralized Management on the Manager.
- Enable Centralized Management on the Entity.
- Add the Entities to the Manager.

Enable Centralized Management on the Manager

To enable Centralized Management and configure the Manager device:

1. Log in to the Manager system.
2. Select **Configuration > Network > Interfaces**.
3. Select the **Centralized Management** check box for the required interface.



Interface 1 - ACTIVE / 1000baseTX <full-duplex> / 00:0c:29:62:92:34 / em0

IP address: 10.0.0.1

Netmask: 255.255.255.0

Media: Auto select

Large MTU: ☑

Respond to Ping and ICMP Redirect: ☑

Trusted Subnet: □

Admin & Web User Login: ☑

WebMail: ☑

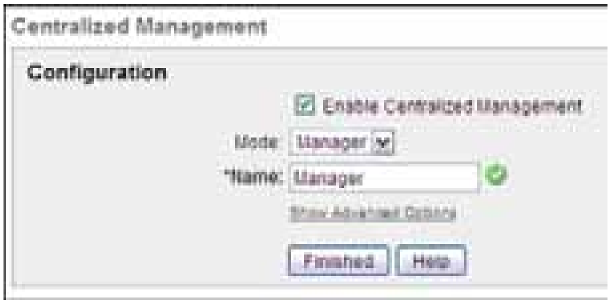
SNMP Agent: □

Centralized Management: □

HTTP/HTTPS Proxy: □

4. Click **Apply**.

   You must restart the system.
5. Select **Administration > Multi-System Management > Centralized Management > Configure**.



Centralized Management

Configuration

☑ Enable Centralized Management

Mode: Manager

*Name: Manager

6. Select the **Enable Centralized Management** check box.
7. From the **Mode** drop-down list, select **Manager**.

   This device acts as the single point of management for a Centralized Management Federation of Entities.
8. In the **Name** text box, type a name to identify this device in the CM federation.

   The default name is the device host name.
9. Click **Finished**.

10. Click **Show Advanced Options** to display the key used by this Manager device to authenticate to other Entities in the Federation.

    If you use automatic key exchange (this is the default behavior), there is no additional configuration required. If you use manual key exchange, this Manager key is manually copied to each Entity in the Federation.

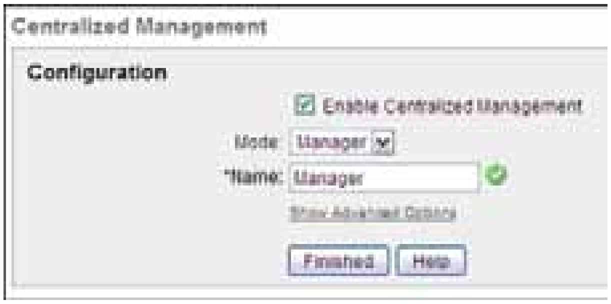
Configure Manager Systems in a Cluster

If the Manager device is configured in a cluster, enable Manager mode on the Primary device. You must also enable the Secondary device in the cluster as a Manager in Centralized Management to make sure that the Secondary system in the cluster can take over as the Manager if the Primary is unavailable.

> **Note** *You must switch all devices to Standalone mode before you configure Centralized Management.*

To configure the Secondary device:

1. Log in to the cluster Secondary system.
2. Change the cluster mode to **Standalone** mode.
3. Select **Configuration > Network > Interfaces**.
4. Select the **Centralized Management** check box for the required interface.
5. Click **Apply**.
   You must restart the system.
6. Select **Administration > Multi-System Management > Centralized Management > Configure**.



Centralized Management

Configuration

☑ Enable Centralized Management

Mode: Manager

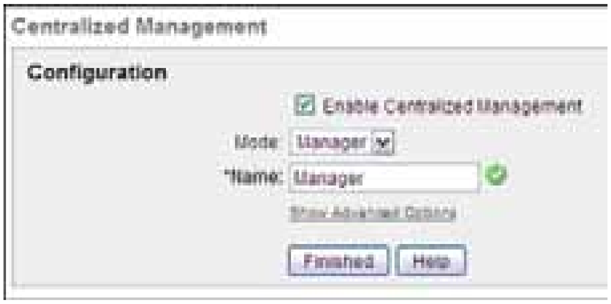
*Name: Manager

7. Select the **Enable Centralized Management** check box.
8. From the **Mode** drop-down list, select **Manager**.
   This Secondary device becomes the Manager if the Primary Manager is unavailable.
9. In the **Name** text box, type a name to identify this device in the CM federation.
   The default name is the device host name.
10. Click **Finished**.

To configure the Primary cluster Manager:

1. Log in to the Primary cluster Manager.
2. Change the cluster mode to **Standalone** mode.
3. Select **Configuration > Network > Interfaces**.
4. Select the **Centralized Management** check box for the required interface.

5. Click **Apply**.
   You must restart the system.
6. Select **Administration > Multi-System Management > Centralized Management > Configure**.



Centralized Management

Configuration

☑ Enable Centralized Management

Mode: Manager

*Name: Manager

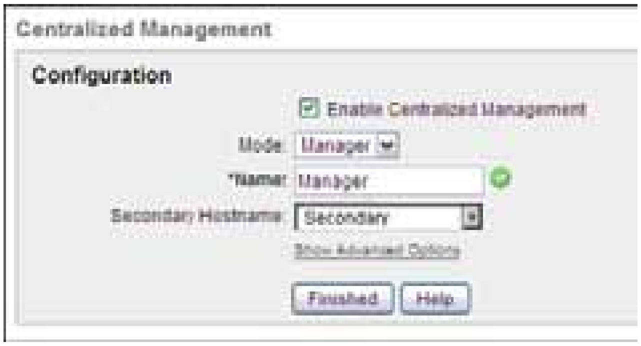
7. Select the **Enable Centralized Management** check box.
8. From the **Mode** drop-down list, select **Manager**.
   This device acts as the single point of management for a Centralized Management Federation of Entities.
9. In the **Name** text box, type a name to identify this device in the CM Federation.
   The default name is the device host name.
10. Click **Finished**.

Now you must switch both devices back to their original Cluster mode top make sure they are properly configured and licensed as Centralized Management Managers before you cluster the devices and add Entities to the Federation.

1. Log in to the Primary and change the cluster mode of the Primary from **Standalone** mode to **Primary** mode.
2. Log in to the Secondary system and change the cluster mode of the Secondary system from **Standalone** mode to **Secondary** mode.

   After you change the cluster mode, the Centralized Management menu items no longer appear on the Secondary. Any Centralized Management configuration performed on the Primary is automatically replicated to the Secondary system.

3. On the **Primary**, select **Administration > Multi-System Management > Centralized Management > Configure**.
4. From the **Secondary Hostname** drop-down list, select the **Secondary** device in the cluster and click **Finished**.
   This device becomes the Manager system if the Primary is unavailable.



Centralized Management

Configuration

☑ Enable Centralized Management

Mode: Manager

*Name: Manager

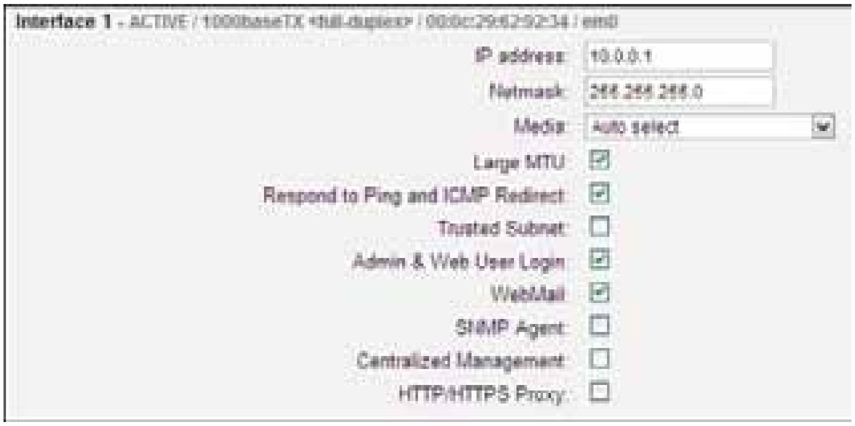
Secondary Hostname: Secondary

The cluster Manager setup is now complete. Proceed to the next section to add Entity systems to the Federation.

Enable Centralized Management on Entity systems

To enable Centralized Management on each Entity in the Federation:

1. Log in to the Entity system.
2. Select **Configuration > Network > Interfaces**.
3. Select the **Centralized Management** check box for the required interface.



Interface 1 - ACTIVE / 1000baseTX <full-duplex> / 00:0c:29:62:92:34 / em0

IP address: 10.0.0.1

Netmask: 255.255.255.0

Media: Auto select

Large MTU: ☑

Respond to Ping and ICMP Redirect: ☑

Trusted Subnet: □

Admin & Web User Login: ☑

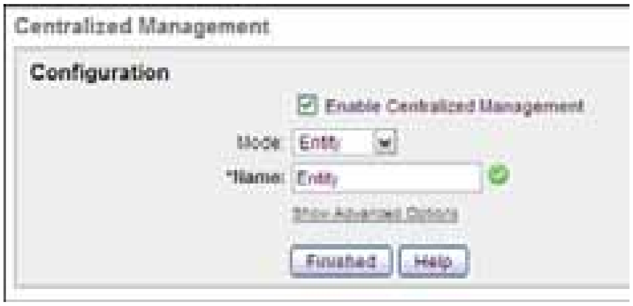
WebMail: ☑

SNMP Agent: □

Centralized Management: □

HTTP/HTTPS Proxy: □

4. Click **Apply**.
   You must restart the system.
5. Select **Administration > Multi-System Management > Centralized Management > Configure**.
6. Select the **Enable Centralized Management** check box.



Centralized Management

Configuration

☑ Enable Centralized Management

Mode: Entity

*Name: Entity

7. From the **Mode** drop-down list, select **Entity**.

   This device acts as an Entity in a Centralized Management Federation. You can monitor and manage this device from the Manager. If this Entity is clustered, select the **Secondary** address from the drop-down list. The Secondary take over for the Primary Entity if it is unavailable.

   You do not need to enable Centralized Management on other devices in the cluster (for example, Secondary and Client devices). They receive their CM configuration from the Primary Entity in the cluster.

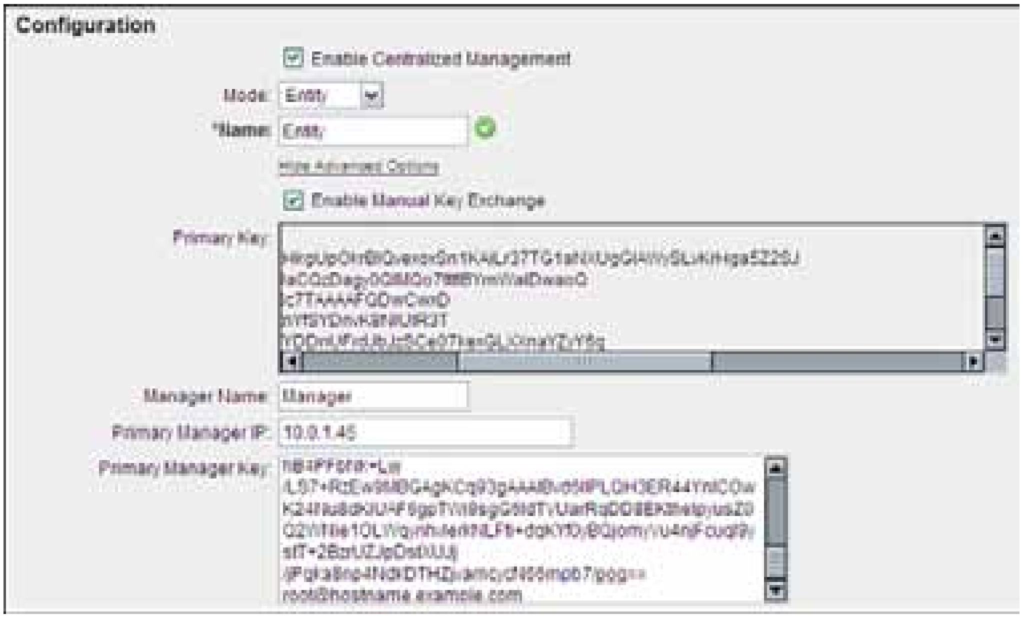
8. In the **Name** text box, type a name to identify this system in the CM Federation.
   The default name is the device host name.

9. Click **Finished**.

   To add the Entity to the Centralized Management Federation, you must add the device to the Entity configuration on the Manager, as described in the next section.

10. Click **Show Advanced Options** to reveal the configuration items for manual key exchange between the Manager and Entity systems.

    The Manager and Entity systems in the Federation use automatic key exchange by default for authentication. Manual key exchange allows you to manually copy the key values between the Manager and Entity devices to troubleshoot key exchange issues.



Configuration

☑ Enable Centralized Management

Mode: Entity

*Name: Entity

☑ Enable Manual Key Exchange

Primary Key: [illegible]

Manager Name: Manager

Primary Manager IP: 10.0.1.45

Primary Manager Key: [illegible]
root@hostname.example.com

- **Enable Manual Key Exchange** – Select the check box to enable manual key exchange.
- **Primary Key** – This is a static value that displays the key for this specific device. This Entity's key is copied to the Manager.
- **Manager Name** – Type the name of the Manager.
- **Primary Manager IP** – Type the IP address of the Primary Manager.
- **Primary Manager Key** – Copy the key from the Primary Manager and paste it into the text box.
- **Secondary Manager IP** – If the Manager is clustered, type the IP address of the Secondary that takes over as the Manager if the Primary is unavailable.
- **Secondary Manager Key** – Copy the key from the Secondary Manager and paste it in the text box.

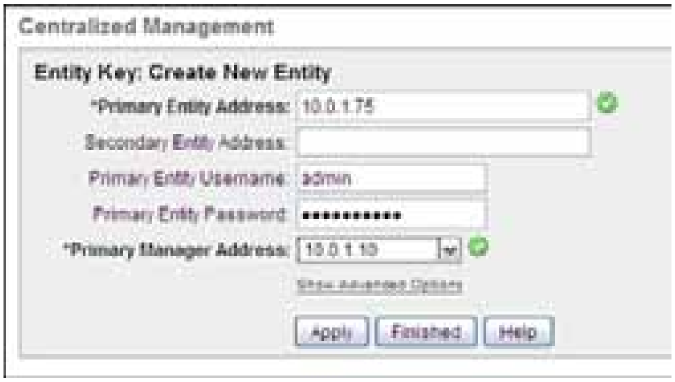
Add Entities to a Federation on the Manager System

To add new Entities to the Centralized Management Federation:

> ***Note*** *You must enable and initialize Centralized Management on Entities before you add them to the Federation on the Manager.*

Log in to the Manager system.

1. Select **Administration > Multi-System Management > Centralized Management > Entities**.
2. Click **Create New Entity**.



Centralized Management

Entity Key: Create New Entity

*Primary Entity Address: 10.0.1.75

Secondary Entity Address:

Primary Entity Username: admin

Primary Entity Password: ●●●●●●●●●●●

*Primary Manager Address: 10.0.1.10

3. In the **Primary Entity Address** text box, type the IP address of the Primary Entity.
   If the Entity is located behind a NAT device, for example, a network firewall, type the public address of the NAT device.
4. In the **Secondary Entity Address** text box, type the Secondary Entity address if this device is clustered.
5. In the **Primary Entity Username** text box, type the admin user for the device.
   This is the administrative user for this system.
6. In the **Primary Entity Password** text box, type the password for the admin user.
7. From the **Primary Manager Address** drop-down list, select the IP address of the Primary Manager device.

   This is the IP address of the Manager in the Federation. If Centralized Management is used in a cluster, select the Secondary Manager address from the drop-down list. If the Manager is located behind a NAT device, for example, a network firewall, select **Specify** from the drop-down list and type the public address of the NAT device.

8. Click **Apply**.
9. Click **Finished**.
10. Click **Show Advanced Options** to reveal the configuration items for manual key exchange. Manual key exchange allows you to manually copy the key values between the Manager and Entity devices to troubleshoot key exchange issues.

    - **Enable Manual Key Exchange** – Select the check box to enable manual key exchange.
    - **Entity Name** – Type the name of the Entity system.
    - **Primary Entity Key** – Copy the key from the Primary Entity system and paste it in the text box.
    - **Secondary Entity Key** – If this Entity is clustered, copy the key from the Secondary Entity and paste it in the text box.

Configuration Sets

Centralized Management allows you to create a global configuration set and apply it to the devices participating in the Centralized Management Federation.

The configuration set includes most aspects of the configuration which can be distributed to Entities in the Federation. This includes message delivery settings, policies, policy mappings, and mail routes. Items unique to each device, for example, the network configuration, are not included.

> ***Note*** *You can only apply a single global configuration set at any one time.*

When you synchronize the configuration set with the Federation for the first time, the configuration set replaces the current local configuration on all Entities in the Federation. Administrators of the Entity systems can modify their local configuration as required to allow for any unique local requirements. Any subsequent configuration sets applied to the Entity only override local values that are not modified.

Click the **Purge Local Settings** link in the menu bar to purge and replace the local Entity configuration.

Configuration Set Features

You can customize and replicate these features in a configuration set:

Category	Configuration Item
Configuration	Directory Servers and Users
	LDAP Aliases, Mapping, Recipients, Relay, Routing
	Alarms
	Customization
	SNMP
	External proxy server
Mail	Mail Access
	Mail Delivery
	Aliases
	Routing
	Mapping
	Virtual Mapping
	Archiving
	DomainKeys
Encryption	
	External Encryption
	SecureMail Encryption
	PostX Encryption
	TLS Encryption
Web Proxy	HTTP/HTTPS Proxy Server
	URL Categorization
	Reputation Enabled Defense

Category	Configuration Item
	Traffic Accelerator
	User Reporting
	URL Block Lists
	Proxy Auto Configuration
Intercept	Intercept Settings
	Connection Control
	Threat Prevention
	Anti-Spam and Brightmail
	Anti-Virus and Spyware
	Outbreak Control
	Malformed Mail
Content Control	Attachment Control
	Content Control
	Content Scanning
	Document Fingerprinting
	Objectionable Content Filter
	Pattern Filters
	Content Rules
	Dictionaries and Lists
Policy	Policies (Policies are accepted as a whole, and individual parts of a policy cannot be overridden locally)
	User, Group, IP, Time, and Domain Policies
User Accounts	Mirror Accounts
	Trusted/Blocked Senders
	User Spam Quarantine
	Remote Authentication
Reports	Reports
	Reports and Logging configuration

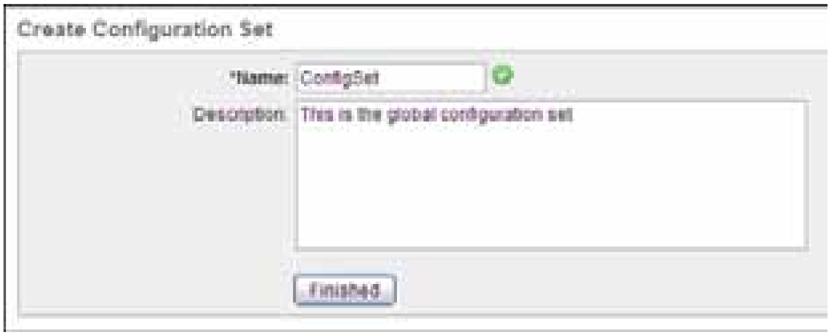
These features are unique to a specific host device and you cannot define them in a configuration set:

Category	Configuration Item
Configuration	Network Settings
	Virtual Interfaces
	Performance Settings
	Static Routes
	Web Server
	Queue Replication
Intercept	Token Analysis Advanced Settings
User Accounts	Admin Account
	Local Accounts
	Relocated Users
	POP3 & IMAP
	SecurID
Management	Backup & Restore (Target names require a variable by the hostname, for example, `%q`)
	Daily Backup
Web Proxy	Proxy Auto Configuration

Create a Configuration Set

To create a Centralized Management configuration set:

1. Log in to the Manager system.
2. Select **Administration > Multi-System Management > Centralized Management > Configuration Set**.
3. Click **Create New Configuration Set** or click the **Configure** link to edit an existing configuration set.



Create Configuration Set

*Name: ConfigSet

Description: This is the global configuration set

4. In the **Name** text box, type a name for this configuration set.
5. In the **Description** text box, type a detailed description for this configuration set.
6. Click **Finished**.

> ***Note*** *The name "Global" is a reserved word and cannot be used. The name "Global" appears as the name of the configuration set on all Entity devices.*

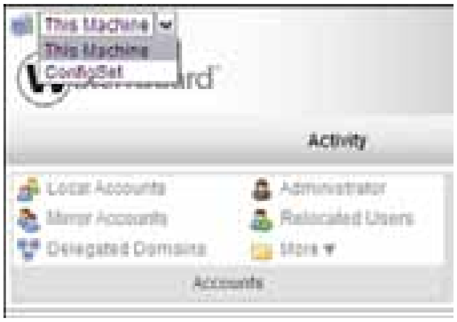
Define a Configuration Set

To select and define a configuration set:

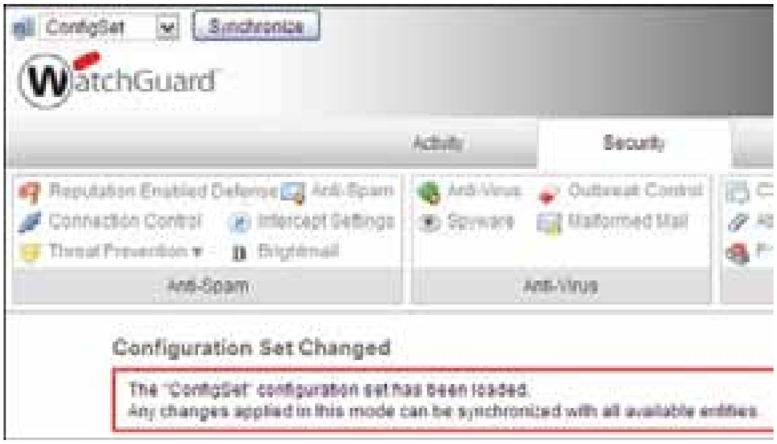
1. Log in to the Manager system.
2. From the drop-down list, select a configuration set.

   For example, **ConfigSet**.

   The initial context in the drop-down list is **This Machine**. This context indicates the current local configuration of the device.

   When you select a configuration set, the page indicates the current loaded configuration set.

   Configuration Set Changed

   The "ConfigSet" configuration set has been loaded.
   Any changes applied in this mode can be synchronized with all available entities.

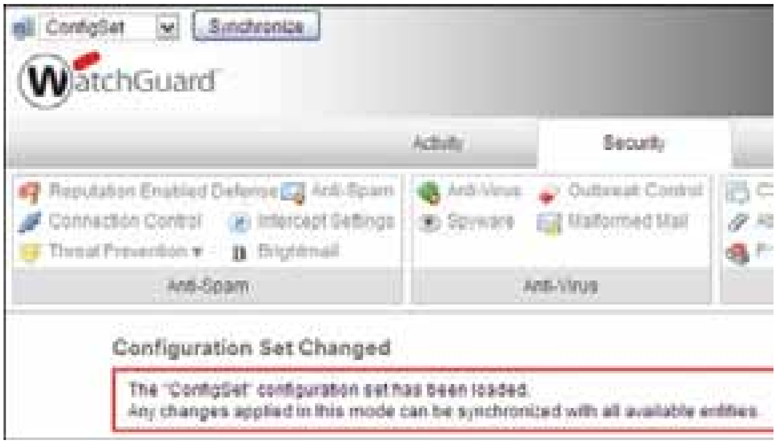
   You can now customize the configuration as required using the displayed menu items.
   This configuration is only saved for this specific configuration set. Only a subset of the main menu appears. This menu displays only configuration parameters that can be replicated to Entities in a Federation.

3. Select **This Machine** from the drop-down list to exit the configuration set and return to the original configuration menu for the Manager.

Apply a Configuration Set

To apply a configuration set to the Entities in the Federation:

1. Log in to the Manager system.
2. Select the configuration set to replicate from the drop-down list, for example, **ConfigSet**.



Configuration Set Changed

The "ConfigSet" configuration set has been loaded.
Any changes applied in this mode can be synchronized with all available entities

3. Click **Synchronize**.

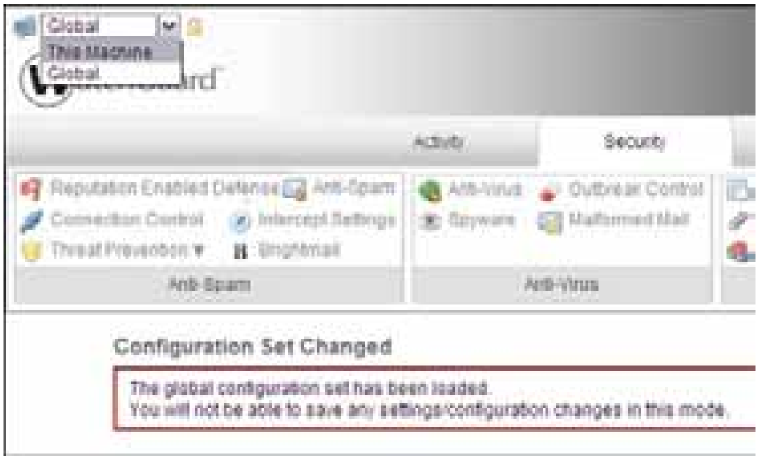
   The configuration set is synchronized with all Entities and the Manager device in the Federation. A message appears that indicates that you cannot use the device until the synchronization is complete.

   > ***Note*** *Make sure each Entity in the Federation is running the same software level (this includes any applicable software updates), before you synchronize a configuration.*

View a Configuration Set on an Entity

To view the configuration settings in the Global configuration set:

1. Log in to the Entity.
2. Select **Global** from the drop-down list.
   The display indicates that the global configuration is loaded.



Configuration Set Changed

The global configuration set has been loaded.
You will not be able to save any settings/configuration changes in this mode.

The Global configuration set appears as **Read Only**. This indicates that only the Manager can modify the Global configuration set. Administrators on the Entity machine can browse the configuration to view what settings apply in the Global configuration set.

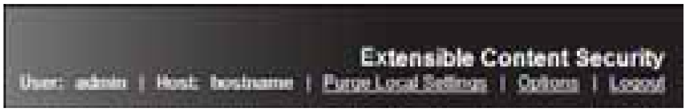
3. To modify the Global configuration set for local requirements, select **This Machine** from the drop-down list.

   In this context, any changes you apply only affect this device. This allows the Entity administrator to modify or extend the Global configuration set with local requirements as needed.

Purge Local Settings

When the Manager in the Federation initially synchronizes a configuration set to this Entity, the configuration set overrides any current local configuration. Any subsequent configuration sets applied to this Entity only override local values that are not modified.

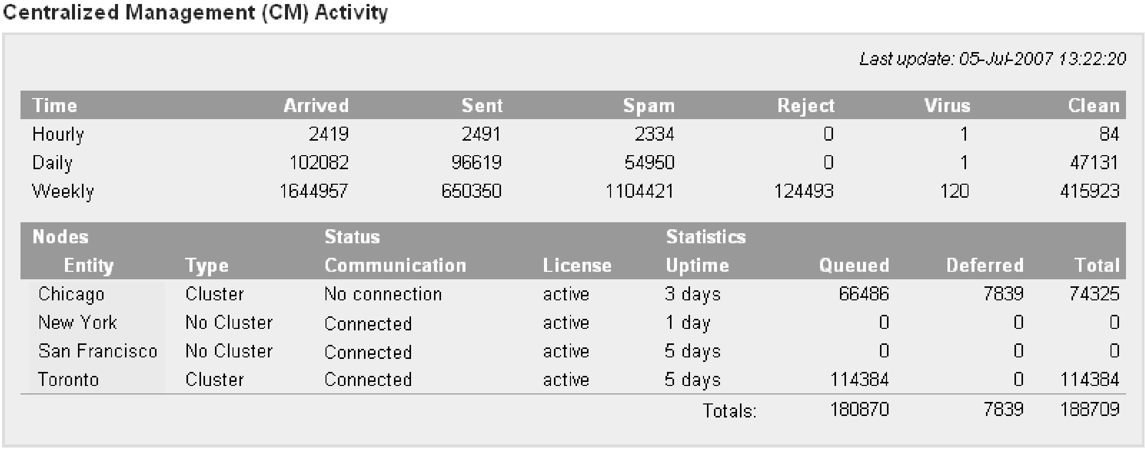
To remove all local configuration overrides and use the current Global configuration set, click **Purge Local Settings** at the top-right of the menu bar.


Extensible Content Security
User: admin | Host: hostname | Purge Local Settings | Options | Logout

A message appears that indicates that you cannot use the device until the purge process is complete.

Centralized Management Activity

To display the Centralized Management Activity page, select **Activity > Status > CM Activity** on the Manager. This page displays the connectivity status and statistics for all Entities in the Federation.



Centralized Management (CM) Activity

Last update: 05-Jul-2007 13:22:20

Time	Arrived	Sent	Spam	Reject	Virus	Clean
Hourly	2419	2491	2334	0	1	84
Daily	102082	96619	54950	0	1	47131
Weekly	1644957	650350	1104421	124493	120	415923

Nodes		Status		Statistics			
Entity	Type	Communication	License	Uptime	Queued	Deferred	Total
Chicago	Cluster	No connection	active	3 days	66486	7839	74325
New York	No Cluster	Connected	active	1 day	0	0	0
San Francisco	No Cluster	Connected	active	5 days	0	0	0
Toronto	Cluster	Connected	active	5 days	114384	0	114384
				Totals:	180870	7839	188709

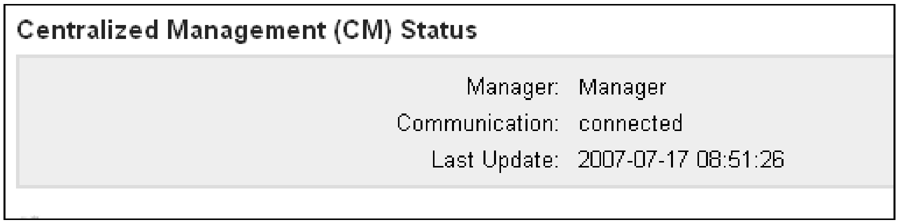
- **Entity** – Displays the Entity name.
- **Type** – Describes the type of Entity. For example, “Cluster” or “No Cluster”.
- **Communication** – Indicates the current status of the Entity. For example, “Connected”.
- **License** – Indicates whether this device has an active system license and the software version.
- **Uptime** – Displays how long the device has been running since the last restart.
- **Queued** – Displays the number of messages currently queued for delivery on the Entity.

- **Deferred** – Indicates the number of messages on the Entity that have had their delivery deferred because the destination mail server is unavailable. The device attempts to deliver these messages at a later time.
- **Total** – Displays the total number of messages currently queued for delivery or deferred on the Entity.

Entity Status

To view the status of an Entity, select **Administration > Multi-System Management > Centralized Management > Entity Status**.

The status displays the name of the Manager system of the Federation, the communications status of this Entity, and the time of the last communication between the Manager and Entity.



Centralized Management (CM) Status

Manager:	Manager
Communication:	connected
Last Update:	2007-07-17 08:51:26

Centralized Management Reports

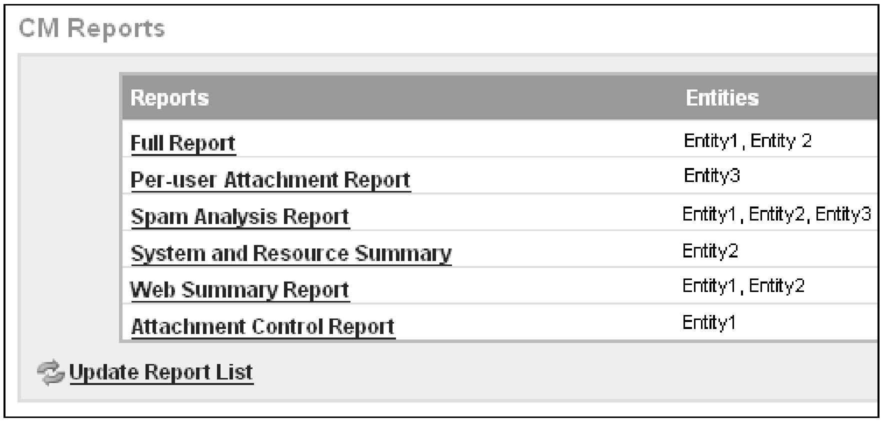
When you use Centralized Management, the Manager can view reports generated on other Entities in the Federation. This allows you to view and manage reports from one central location, and you do not have to login to each Entity to view its reports.

You can also search the Message History of all Entities in the Federation from the Manager and view the results without having to log in to each Entity.

View Centralized Management Reports

To view Centralized Management reports:

1. Log in to the Manager system.
2. Select **Activity > Reports > Centralized Management**.
   The CM Reports page displays the available reports and indicates which Entities have generated the reports.



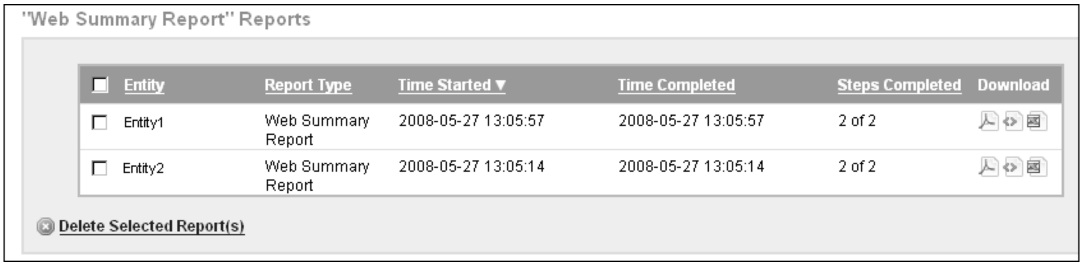
CM Reports

Reports	Entities
Full Report	Entity1 , Entity 2
Per-user Attachment Report	Entity3
Spam Analysis Report	Entity1 , Entity2, Entity3
System and Resource Summary	Entity2
Web Summary Report	Entity1 , Entity2
Attachment Control Report	Entity1

3. To refresh the Entity report list with any new generated reports, click **Update Report List**.
4. Click a report to view the reports for each Entity that has generated that type of report.

   For example, **Web Summary Report**.

   From this page you can view and manage the generated reports for each Entity. To delete a report, select the Entity report, and then click **Delete Selected Reports**.



"Web Summary Report" Reports

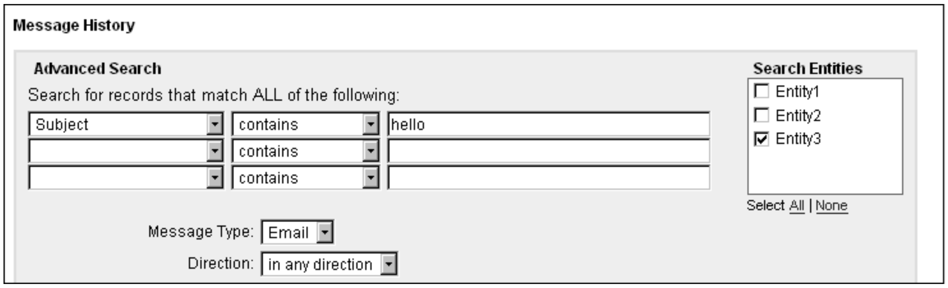
□ Entity	Report Type	Time Started ▼	Time Completed	Steps Completed	Download
□ Entity1	Web Summary Report	2008-05-27 13:05:57	2008-05-27 13:05:57	2 of 2	
□ Entity2	Web Summary Report	2008-05-27 13:05:14	2008-05-27 13:05:14	2 of 2	

View Message History

You can search the Message History across all Entities in the Federation from the Manager device. This includes all search criteria and advanced search parameters.

To search the Message History of Entities in the Federation:

1. On the Manager, select **Activity > History > Message History**.
   A list of Entities appears in the right-side box.



Message History

Advanced Search

Search for records that match ALL of the following:

Subject	contains	hello
	contains	
	contains	

Message Type: Email

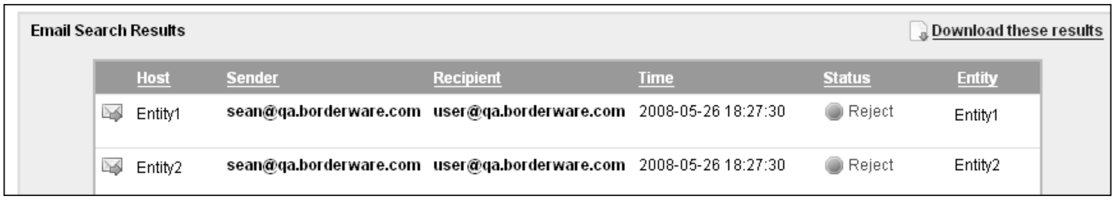
Direction: in any direction

Search Entities

□ Entity1
□ Entity2
☑ Entity3

2. Select the Entities on which you want to perform the message history search.
3. Enter your search criteria, and then click **Search**.

   The **Entity** column identifies the Entity device on which the search results appeared.



Email Search Results

Host	Sender	Recipient	Time	Status	Entity
Entity1	sean@qa.borderware.com	user@qa.borderware.com	2008-05-26 18:27:30	● Reject	Entity1
Entity2	sean@qa.borderware.com	user@qa.borderware.com	2008-05-26 18:27:30	● Reject	Entity2

By default, the results are sorted by Entity. You can also sort by other criteria, for example, host name or date.

19 Reports and Logs

About Reports

The WatchGuard XCS reporting functions provide a comprehensive range of informative reports:

- Full Email Report
- Email Executive Summary
- Virus Report
- Spyware Report
- Traffic Report
- Email Analysis Report
- Intercept Report
- Attachment Control Report
- Per-user Attachment Report
- Pattern / Filter Report
- Outbound Content Control Report
- Connection Control Report
- User / Host Report
- Session Summary
- Reputation Domain Report
- Rules Report
- System and Resource Summary
- Web Analysis Report
- Web Summary Report
- Web User Summary Report

You can generate reports on demand and at scheduled times. The reports data is derived from information written to the message logs and stored in the reporting database. You can store and view up to a month's reporting data, depending on message loads for your particular environment.

Note *The XCS device automatically adjusts the number of days of reporting data that can be stored based on current device resources.*

Reports are stored on the system for online viewing, and can also be emailed automatically to the administrator. Reports can be generated in PDF (Adobe Portable Document Format), CSV, and HTML format. In clustered environments, reports generate information aggregated for the entire cluster. System and resource reports display information for each host in the cluster. In Centralized Management environments, the Manager system can configure and view reports for all Entities in a Centralized Management Federation.

Domain Reporting

For organizations that support multiple domains, you can add per domain information to specific reports to provide you with statistics for each domain hosted by the WatchGuard XCS. You can also enable domain reports that create separate reports for each hosted domain. These domain reports can be emailed to the specific administrator of each domain.

> **Note** *Per Domain and Hosted Domain reports are not available for all report types. See Report Types for detailed information on the data that is generated for each report type.*

Inbound and Outbound Reporting

In most cases, inbound messages are considered untrusted, and outbound messages are considered trusted. For any of the recipient-based reports, the inbound or outbound status is determined by mail routes during message processing. For domain-based reports, you can upload a list that contains hosted domains and their administrative email addresses in **Security > Content Control > Dictionaries & Lists**. In this case, inbound and outbound determinations are based on the sender and recipient of the message.

For example, for a list of the hosted domains example1.com and example2.com:

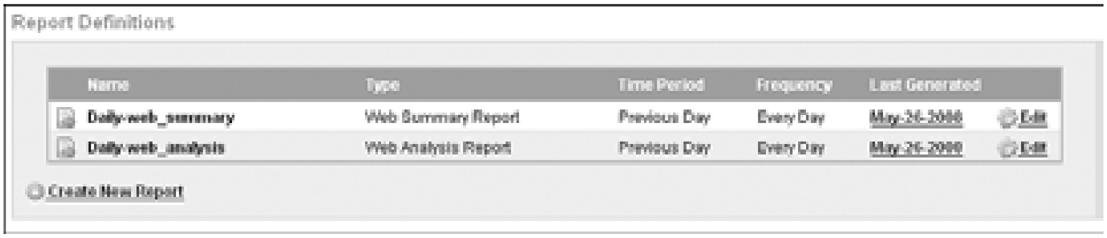
- Inbound mail for example1.com is based on the recipient domain being example1.com
- Outbound mail for example1.com is based on the sender domain being example1.com
- These same rules apply for example2.com, but mail from example1.com to example2.com is counted as outbound for example1.com and inbound for example2.com

> **Note** *When you create Hosted Domain outbound reports, make sure that the uploaded domain name is the domain of the Sender. Inbound reports use the domain of the Recipient.*

Schedule Reports

To schedule and generate reports:

1. Select**Activity>Reports>Schedule**.



Report Definitions

Name	Type	Time Period	Frequency	Last Generated	
Daily-web_summary	Web Summary Report	Previous Day	Every Day	May-26-2008	Edit
Daily-web_analysis	Web Analysis Report	Previous Day	Every Day	May-26-2008	Edit

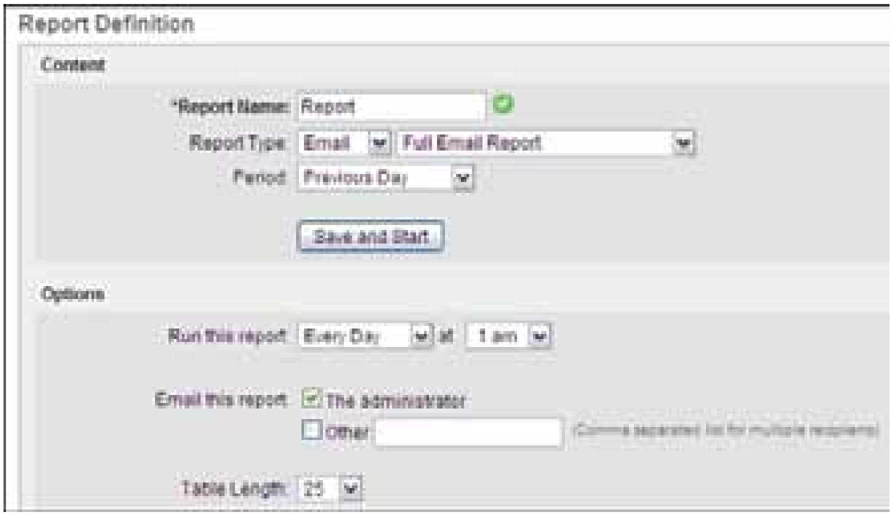
The *Report Definitions* page displays any scheduled and defined reports. This includes the report name, report type, the reporting time period, the frequency, and the last time the report was generated.

2. Click the **Edit** link to edit an existing report, or click the **Create New Report** link to create a new report definition.
3. To view the last generated report from this report definition, click the **Last Generated** date link.

Create a New Report

To create a new report:

1. Click the **Create New Report** link.
   The Report Definition page appears.



Report Definition

Content

*Report Name: Report

Report Type: Email | Full Email Report

Period: Previous Day

Save and Start

Options

Run this report: Every Day at 1 am

Email this report: ☑ The administrator

□ Other (Comma separated list for multiple recipients)

Table Length: 25

2. In the **Report Name** text box, type a descriptive name for this report.
   The name must only contain alphanumerical letters, numbers, and spaces, and must not contain any special characters.
3. From the **Report Type** drop-down list, select the which type of report to run.

   Select a category of reports, for example, **Email**, **Web**, and **System**, and then choose a report sub-type for that category.
4. From the **Period** drop-down list, select the time period for the report coverage:
   - **Previous Day** (includes up to midnight of the previous day)
   - **Last 7 Days**
   - **Sunday - Saturday** (includes 7 days from a Sunday to the next Saturday)
   - **Monday - Friday** (includes 5 days from Monday to Friday)
   - **Previous Month** (this is the previous calender month).

> ***Note*** *To report on the previous month in a report definition, the Reporting Summary Days option in **Configuration > Miscellaneous > Reports** must be set to 60 days or more to have enough data to cover the previous month time period.*

5. From the **Run this report** drop-down list, select the day and time to run the scheduled report.
6. In the **Email this report** section, select who to send a copy of the report to when it is generated.

   Select **The administrator** to send it to the administrator of this system, and/or select **Other** and enter a comma separated list of addresses to which to send the report.

   For example,

   `admin@example.com,admin2@example.com,admin3@example.com`
7. From the **Table Length** drop-down list, select the length for each report field.

   For example, in the Top Viruses list, the top 50 viruses are displayed if this field is set to 50. The default is 25. You can configure the default value in **Configuration > Miscellaneous > Reports**.
8. Click **Save and Start** to save the report and generate it immediately.

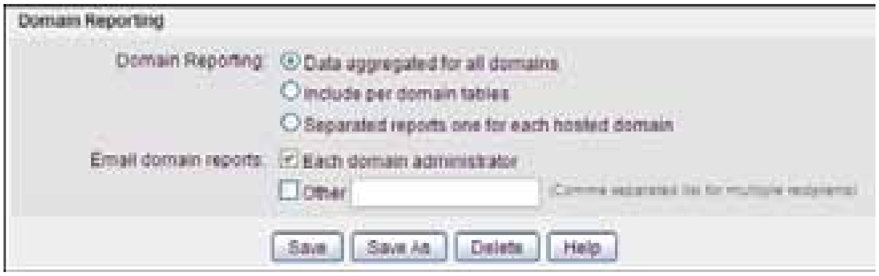
   Select **Save** or **Save As** (to save under a different name) to save the report and run it at the scheduled time and day.

   Click **Delete** to remove this report definition. Any reports associated with this report definition are not deleted and can still be viewed.

Domain Reports

The Domain Reporting option allows specific reports to be generated and customized for systems that accept messages for multiple domains. To upload a list of hosted domains and associated domain administrator email addresses, select **Configuration > Miscellaneous > Reports**.

> ***Note*** *When you upload hosted domains, statistics collection on these domains begin from that point and may not be immediately available for reports.*



Domain Reporting

Domain Reporting: ● Data aggregated for all domains
○ Include per domain tables
○ Separated reports one for each hosted domain

Email domain reports: ☑ Each domain administrator
□ Other (Comma separated list for multiple recipients)

These options are available:

Data aggregated for all domains

This option generates reports based on all message domains hosted by this system. The reports do not break down any report statistics based on each domain, but report on all messages as a whole for this system. This is the default setting.

Include per domain tables

This option generates the system reports, but includes tables displaying a summary of the messages based on each domain hosted by the system. For example, if you run a Full Email Report, only one Full Email Report is generated, but it includes statistics on each domain in separate tables in the report.

Separated reports one for each host domain

This option generates the system reports, but creates a separate report for each domain hosted by the system. For example, if you run a Full Email Report, a Full Email Report is generated separately for each domain on the system.

> **Note** *Per Domain and Hosted Domain reports are not available for all report types. See Report Types for detailed information on the data that is generated for each report type.*

Email Domain Reports

Select to whom a copy of the report are sent to when the report is generated. Select **Each domain administrator** to send the report to the administrator of each domain, and/or select **Other** and enter a comma separated list of addresses to which to send the report.

For example:

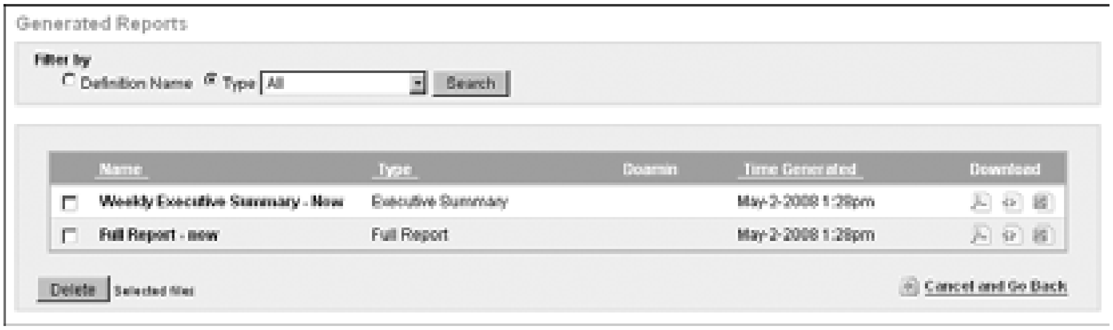
`admin@example.com,admin2@example.com,admin3@example.com`

If a separate report is run for each domain, the domain administrator only receives the report for their own domain.

View Reports

To view your generated reports:

1. Select **Activity > Reports > View**.
   The Generated Reports page appears.



	Name	Type	Doamin	Time Generated	Download
□	Weekly Executive Summary - Now	Executive Summary		May-2-2008 1:28pm	
□	Full Report - now	Full Report		May-2-2008 1:28pm	

   Reports are generated in PDF (Adobe Portable Document Format), CSV, and HTML format.

2. Click the appropriate icon to view the contents of the report in the specified format.
   The report either appears in a new browser window (for an HTML report) or you can save the PDF and CSV versions of the report on the local computer.

> **Note** *HTML reports are optimized for on-screen viewing, and are not recommended for printing reports. The PDF report type should be used for report printing.*

   You can filter the generated reports page by report definition name or by the type of report using the drop-down list of available report names or definitions.

3. Click **Search** to filter the reports list.

Report Types

Full Email Report

Includes the highlights from all listed Email report types. Individual reports may have more detailed information that are not found in the Full Email Report. This report does not include Web Proxy statistics. You can generate Per-domain and hosted domain reports with this report.

Email Executive Summary

The Email Executive Summary provides an overview of mail processing statistics for inbound and outbound mail. You can generate hosted domain reports with this report.

- **Inbound Message Summary** – Indicates the number of inbound messages that are rejected, classified as spam, caught by content control, contained viruses, or are clean.
- **Rejected** – Indicates the number of messages rejected by Reputation Enabled Defense and other features that reject a message before the SMTP connection is complete. This category is displayed for inbound mail only. This statistic includes these connection rejects: Reputation Enabled Defense Connection Reject (Reputation, Infection, and Dial-up), DNS Block List Reject, Threat Prevention Reject, Specific Access Pattern Reject, Pattern Filter reject, Connection Rule reject, Reject on unauthorized SMTP pipelining, Reject on unknown sender domain, Reject on missing reverse DNS, Reject on missing sender MX, Reject on non FQDN sender, Reject on Unknown Recipient, Reject on missing addresses, Reject if number of recipients exceeds maximum, Reject if message size exceeds maximum.

> ***Note*** *The bar graph on the right side of the report only indicates rejected messages for Reputation Enabled Defense feature only, and does not include other SMTP connection rejects.*

- **Detected Spam** – Indicates the number of messages that are classified as spam. This includes Certainly Spam, Probably Spam, Maybe Spam, Brightmail spam, Reputation Enabled Defense Spam, and DNS Block List Spam. This category is displayed for inbound mail only. This category also depends on the Spam logging configuration in **Configuration > Miscellaneous > Reports**. The spam action of **Just Log** are counted in the total if enabled in the spam logging configuration.
- **Content Filters** – Indicates the number of messages that had illegal content detected by the Content Control features (Attachment Control, Content Scanning, Pattern Filters, Content Rules, Document Fingerprinting, and Objectionable Content Filtering).
- **Detected Viruses** – Indicates the amount of messages that contained viruses, spyware, or were malformed.
- **Clean** – Indicates the number of messages that are processed by the system and passed all security, spam, and content checks. This includes messages that are detected by these features but have an action of **Just Log**.
- **Total** – The total number of messages.
- **Outbound Message Summary** – Indicates the number of outbound messages that have had their content detected by the Content Control features (Objectionable Content Filter, Attachment Control, Content Scanning, Pattern Filters, Content Rules, Document Fingerprinting) and Clean mail.

- **Inbound Rejected Connections** – Indicates the number of messages are rejected during the SMTP connection by Reputation Enabled Defense and other connection-level reject features, for example, Specific Access Patterns.

Virus Report

Includes information on inbound and outbound viruses, lists of top viruses, and top virus senders. You can generate hosted domain reports with this report.

- **Inbound Viruses** – Displays the top inbound viruses and the amount of times they were detected. This includes a graph showing the thousands of viruses detected per hour.
- **Recent Inbound Virus Details** – Displays the most recent inbound virus-infected messages. This includes the Queue ID, Time Received, Sender, Recipient, and Virus Name.
- **Outbound Viruses** – Displays the top outbound viruses and the amount of times they were detected. This includes a graph showing the thousands of viruses detected per hour.
- **Recent Outbound Virus Details** – Displays the most recent outbound virus-infected messages. This includes the Queue ID, Time Received, Sender, Recipient, and Virus Name.
- **All Outbound Virus Senders** – Displays information on the top virus senders. This includes the sender email address, virus name, and the number of virus-infected messages sent.

Spyware Report

Provides a chart on the number and types of Inbound and Outbound spyware programs found in Email messages. You can generate hosted domain reports with this report.

- **Inbound and Outbound Spyware Blocking** – Indicates the different types of spyware programs that were detected. A graph indicates the number of spyware programs blocked per hour.
- **Inbound and Outbound Spyware Summary** – Provides a list of the most recent Inbound and Outbound messages that were detected as containing spyware. Includes information on the Queue ID of the message, the time received, the Sender and Recipient addresses, and the name of the spyware program.

Traffic Report

Reports on message volume and connection counts. You can generate per-domain and hosted domain reports with this report.

- **Total Traffic Summary** – Displays the total number of inbound and outbound mail messages. This includes a graph showing the amount of mail in thousands of messages per hour.
- **Total Traffic by Domain** – Indicates the number of inbound and outbound mail messages per domain.
- **Total Traffic Size** – Indicates the total size of inbound and outbound mail messages in MB. This includes a graph showing the amount of mail per hour in MB per hour.
- **Total Size by Domain** – Indicates the total size of inbound and outbound mail messages per domain in MB.
- **Connection Summary** – Displays the number of mail connections to this system that passed or were incomplete (rejected). This includes a graph showing the number of connections in thousand connections per hour.
- **Mail Processing Times** – Indicates for this server the average processing time in seconds for each message. This includes a graph showing the average time in the mail queue in seconds per hour.

Email Analysis Report

Provides an overview of mail traffic analysis by the mail scanning features. You can generate per-domain and hosted domain reports with this report.

- **Inbound and Outbound Message Summary** – A pie chart displays a breakdown of inbound and outbound messages processed based on Reputation Enabled Defense and Connection Rejects, Detected Spam, Content Filters (Attachment Control, Content Scanning, Pattern Filters, Content Rules, Document Fingerprinting, and Objectionable Content Filtering), Detected Viruses (Viruses, Spyware, and Malformed), Clean, and Total Mail messages. A graph displays the thousands of messages per hour based on the type of message.
- **Inbound and Outbound Analysis Details and Recipient Actions** – Displays a pie chart with details of the total number of inbound and outbound messages for each type of message classification (Clean, Attachment Control, Virus, Certainly Spam, Probably Spam, Maybe Spam, and Document Fingerprinting). Also displays a pie chart of the different types of applied recipient actions on inbound and outbound mail (Pass, message was Clean and no action taken, Quarantined, Subject Modified, Reject, and Just Log).

Intercept Component Report

Reports on Intercept Anti-Spam processing. This includes the frequency of spam received based on spam category, the Token Analysis score of messages received, and Intercept component contribution.

- **Spam Frequency** – This graph displays the frequency of Certainly Spam, Probably Spam, and Maybe Spam, received over a period of time.
- **Token Analysis Score** – This graph displays the number of messages received based on their Token Analysis score.
- **Intercept Component Contributions** – This table displays statistics on identified spam for each Intercept component that contributed to the overall Intercept score.

Attachment Control Report

Reports on inbound and outbound attachment types that have been blocked. You can generate per-domain and hosted domain reports with this report.

- **Blocked Attachment Summary** – This table and bar graph displays the Direction, Number of Messages Blocked and Number of Attachments Blocked in both directions and the overall totals.
- **Blocked Attachments by Domain** – If per-domain is enabled, this table displays the domain and number of Inbound and Outbound attachments blocked for the reporting period.
- **Top Blocked Attachments** – Identifies the top blocked attachments for the reporting period.
- **All Outbound Attachments Blocked** – This table displays information on the number of all outbound attachments blocked.

Per-User Attachment Report

The Per-User Attachment Report provides a summary of the number of received and sent attachments, their size in KB, and total number of attachments and total size in KB. These are reported for each domain and each user in the domain. This includes information on the file extension and detected MIME type of all sent and received attachments. You can generate hosted domain reports with this report.

Pattern / Filter Report

Reports on the Inbound and Outbound messages that have matched a Pattern Filter. Hosted domain reports can be generated with this report.

- **Message Filter Rate** – The bar graph displays the thousands of messages per hour that were processed and classified by a Pattern Filter.
- **All Message Filters** – The table displays the Number of Email messages, Filter Number, Name, Action, Pattern, and Comments for all Pattern Filters triggered during the reporting period.

Outbound Content Control Report

Reports on the system's Content Control features indicating the number of occurrences of words found in a dictionary file and the corresponding dictionary line number containing the word. You can generate hosted domain reports with this report.

- **Inbound Content Control Analysis** – The chart displays the breakdown of inbound messages processed based on Pattern Filters, Attachment Control, Content Rules, Objectionable Content, Content Scanning, Clean, and Total messages. A graph displays the thousands of messages per hour for each detected message type.
- **Outbound Content Control Analysis** – The chart displays the breakdown of outbound messages processed based on Pattern Filters, Attachment Control, Content Rules, Objectionable Content, Content Scanning, Document Fingerprinting, Clean, and Total messages. A graph displays the thousands of messages per hour for each detected message type.
- **Top Content Control Occurrences** – The table displays the Number of Occurrences, the File Name and Line Number for any content control dictionaries.

Connection Control Report

The Connection Control report provides information and statistics on inbound and outbound connections for this system. No domain reports are available for this type of report.

- **Connection Control Rate** – A table identifies the connecting host IP addresses and names, the total number of connections from these hosts, and the number of connections that were blocked (before the connection was established). A graph displays the number of Connections per hour to this system, classified by which connections were passed, rejected, and dropped (rejected without notification).
- **Inbound Connection Control** – A table identifies the number of Inbound connections that were passed or were incomplete (Rejected or Dropped), and the combined total of Inbound connections.
- **Outbound Connection Control** – A table identifies the number of Outbound connections that were passed or were incomplete (Rejected or Dropped), and the combined total of Outbound connections.
- **Inbound Rejected Connections** – Provides statistics on the number and types of Inbound connections that were rejected.

User/Host Report

Reports on the top sending hosts, top senders, and top recipients. You can generate hosted domain reports with this report.

- **Top Sending Hosts** – The table displays the Host Name, Host IP, Total Messages, and Total Message size for hosts sending mail to the system.
- **Top Senders** – This table displays the Sender address, Total Messages and Total Size for the top senders during the reporting period.
- **Top Recipients** – This table displays the Recipient address, Total Messages, and Total Size for the top recipients during the reporting period.

Session Summary

The Session Summary report provides a table on WebMail and IMAP logins. No domain reports are available for this type of report.

- **WebMail Usage** – Displays the total number of connected sessions and failed login attempts for WebMail. A graph displays the number of WebMail logins per hour.
- **IMAP Usage** – Displays the total number of connected sessions and failed login attempts for IMAP. A graph displays the number of WebMail logins per hour.
- **IMAP Data Sent** – The amount of IMAP data transferred per hour.

Reputation Domain Report

For each domain processed by this system, this report indicates the amount of Reputation Enabled Defense rejects (messages rejected because the sending system has a poor reputation), the total number of messages, and the Reputation Enabled Defense reject percentage for the domain representing the percentage total of the messages that were rejected due to reputation. Per-domain and hosted domain reports can be generated with this report.

Rules Report

Indicates the number of inbound and outbound messages acted upon by the Content and Connection Rules for specific time intervals. A table of the Top Applied Rules lists the most common triggered rules. This includes information on the rule ID number, name, final action of the rule, condition, description, and the number of times it was triggered.

System and Resource Summary

Reports on CPU, disk, memory, mail queue, and network traffic statistics. In a cluster, separate statistics are provided for each system in the cluster. No domain reports are available for this type of report.

- **CPU Load** – The line graph displays the Average and Peak CPU Load during the reporting period.
- **Disk Capacity** – The table displays the Server, Disk partition, Mount point, KB available, KB total, KB percentage used, I-nodes available, I-nodes total and I-node percentage used at the end of the reporting period.
- **Disk History** – The graph displays the time history for Disk Capacity Percentage Used and I-node Percentage Used for each disk partition over the reporting period.
- **Swap Usage** – The table displays the host name and the Minimum, Average, and Maximum Swap usage (in MB) over the reporting period. The line graph displays the time history for this data.
- **Memory Paging** – The graphs displays time histories for Pages Read and Pages Written over the reporting period.
- **Mail Queue Sizes** – The graphs displays the time histories for Minimum, Average, and Peak for the Mail Queue and Deferred Queue over the reporting period.

- **Network Activity** – A graph displays for each active network device on the system. Each graph shows the time history for MB transferred in and out of a specific interface.

Web Analysis Report

Provides a detailed analysis of Web traffic. No domain reports are available for this type of report.

- **Web Blocked Content** – Displays statistics on each message type that is blocked. This includes URL Categorization, Viruses, Spyware, Content Control (includes OCF, Attachment Control, and Content Scanning), URL Block Lists (UBL), Reputation Enabled Defense, and the Blocked Sites List.
- **Web Cache Efficiency** – Displays the efficiency of the web cache based on the number of cache hits (when content was found in the local disk cache), and the number of web server requests that did not find the data in the disk cache and had to go to the Internet web server to fetch the content.
- **Top Users by Browse Time** – Displays the top users with the most browse time. Email addresses are displayed for users when they have authenticated to the Web Proxy. Unauthenticated or unknown users are identified by their IP address.
- **Top Domains by Visits** – Displays the top web site domains with the most visits and their total browse time.
- **Top Blocked Websites** – Displays the top web sites that were blocked for any content issue. This includes viruses, spyware, Attachment Control, and URL Categorization.
- **Viruses** – Displays the top web sites that were blocked because the downloaded files contained viruses, and the top viruses that were detected in web traffic.
- **Spyware** – Displays the top web sites that were blocked because the downloaded files contained spyware programs, and the top spyware programs that were detected in web traffic.
- **Attachments** – Displays the top blocked sites by attachment type, and the top blocked attachment types.
- **URL Categorization** – Displays the top blocked sites by URL Categorization and top blocked URL Categories. This statistic only appears if URL Categorization is enabled and licensed.
- **Top Blocked Client IP Addresses** – Displays the top client IP addresses that had web content blocked.
- **Top Blocked Users** – Displays the top users that had web content blocked.
- **Top Browsed Categories** – Displays the top browsed categories if URL Categorization is enabled and licensed.
- **RED Traffic Classification** – Displays the number of web sites with good, neutral, and bad reputations.

Web Summary Report

Provides a summary of Web traffic statistics based on the types of messages, connections, and request information. No domain reports are available for this type of report.

- **Web Summary Statistics** – Provides a summary of Web traffic. This includes a breakdown of the count for each type of messages: Total Web Requests, Blocked Viruses, Blocked Spyware, URL Categorization, Content Control (OCF, Attachment Control, and Content Scanning), URL Block Lists, HTTP Blocked Sites, and Reputation Enabled Defense.
- **Web Connection and Requests Stats** – A graph of web connection statistics for the number of active server connections per hour, and the number of HTTP requests (in thousands) per hour.

Web User Summary Report

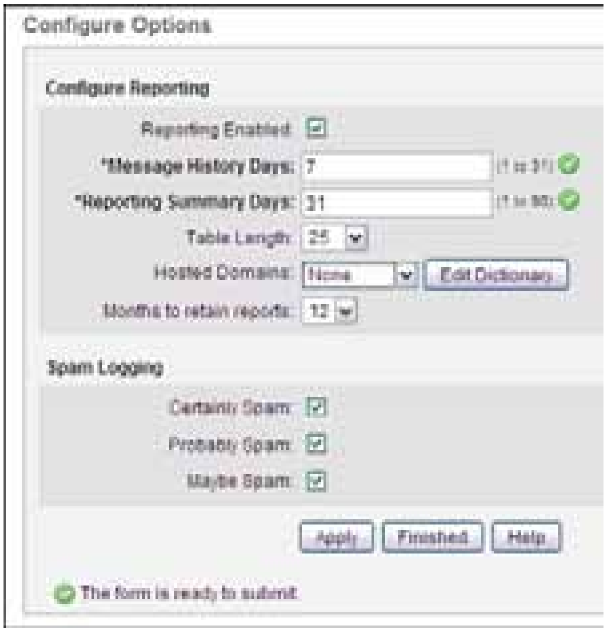
Reports on the web browsing habits of a specific user. Email addresses are displayed for users when they have authenticated to the Web Proxy. Unauthenticated or unknown users are identified by their IP address.

- **Total Browse Time** – Displays the total browse time for the user.
- **Total Domain Visits** – Displays the total domain visits and their browse time for the user.
- **Top Blocked Sites** – Displays the top blocked sites for the user.
- **Top Blocked Categories** – Displays the top blocked categories if URL Categorization is enabled.
- **Top Browsed Categories** – Displays the top browsed categories (by visits) if URL Categorization is enabled.

Configure Reports

To configure global report settings:

1. Select **Configuration > Miscellaneous > Reports**.
   The Configure Options page appears.



Configure Options

Configure Reporting

Reporting Enabled: ☑
*Message History Days: 7 (1 to 31)
*Reporting Summary Days: 31 (1 to 90)
Table Length: 25
Hosted Domains: None
Months to retain reports: 12

Spam Logging

Certainly Spam: ☑
Probably Spam: ☑
Maybe Spam: ☑

The form is ready to submit.

2. Select the **Reporting Enabled** check box.

   The reporting database is populated with information that is obtained by interpreting the system log files. If you disable reporting, no new information is saved in the reporting database. This includes message and system history. We recommend you do not disable reports unless the device is overloaded, or if you are testing performance levels.

3. In the **Message History Days** text box, type the maximum number of days (between 1 and 31) of message history to retain online in the message database.
   Data older than this value is deleted as required. The default is 7 days.
4. In the **Reporting Summary Days** text box, type the maximum number of days (between 1 and 90) of reporting summary information to retain online in the reporting database.

The XCS device automatically adjusts the number of days of reporting data that can be stored based on current system disk resources and message loads. If the number of reporting days is changed by the device, an alarm notifies the administrator. The default is 31 days.

> ***Note*** *To report on the previous month in a report definition, the Reporting Summary Days must be set to 60 days or more to make sure there is enough data to cover the previous month time period.*

5. From the **Table Length** drop-down list, select the length for each report field.

   For example, in the *Top Viruses* list, the top 50 viruses are displayed if this field is set to 50. This value can be changed for specific fields within the report configuration itself. The default is 25.

6. The **Hosted Domains** option allows you to select a list of domains and hosted domain admin email addresses hosted by this WatchGuard XCS that are included in the Domain reports. Domain reports can be emailed to the specified domain administrator address.

   These lists are created in **Security > Content Control > Dictionaries & Lists**. See *Dictionaries and Lists* for more details on creating lists.

   Use the List type **Domain&Email** and use the format `domain,email`.

   For example,

   ```
   example.com,admin@example.com
   ```
   ```
   example2.com,admin@example2.com
   ```
   ```
   example3.com,admin@example3.com
   ```

   You can upload a maximum of 250 domains. After you upload and select the file, domain reports can be generated when creating a new report definition.

7. From the **Months to Retain Reports** drop-down list, select the number of months to retain generated reports. The default is 12 months.
   Reports older than the selected time period are deleted.

Spam Logging

The spam logging options modify the behavior of how the reporting engine calculates statistics for messages that have a **Just Log** Intercept action applied for the **Certainly Spam**, **Probably Spam**, and **Maybe Spam** categories.

If you enable this option, for each category where the Intercept action is **Just Log** (as configured in **Security > Anti-Spam > Anti-Spam**), the message is counted as spam for reporting purposes. If you disable this option, messages that have the **Just Log** action applied are counted as clean in reports and the Dashboard statistics.

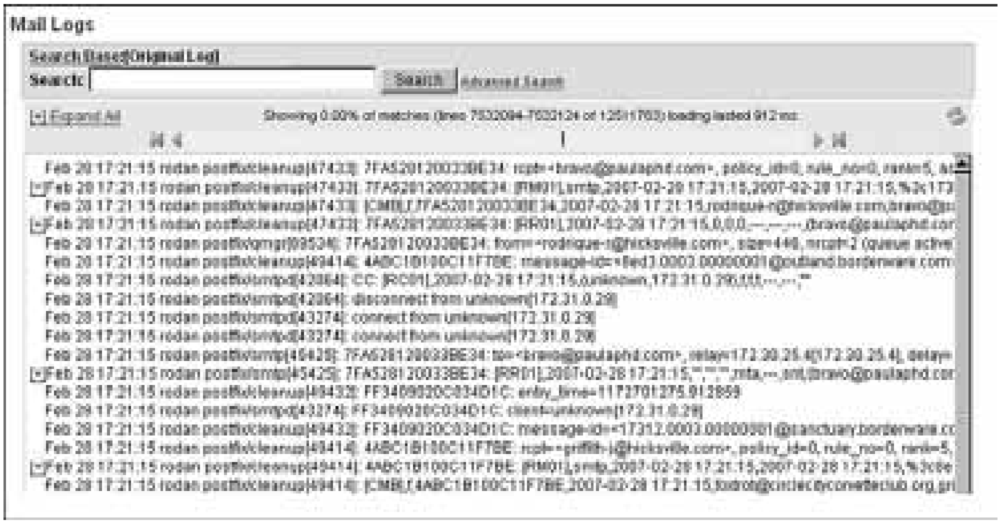
Mail Logs

The Mail Logs are the most important and informative logs to monitor because they contain a record of all mail messages processed by the system.

To access the WatchGuard XCS mail logs:

1. Select **Activity > Logs > Mail**.
   The Mail Logs page appears and displays the end of the log file.
2. Use the slider control to page through the log file, or use the right and left arrow icons.

   You can also jump to the start or end of the log file using the arrow icons as required.

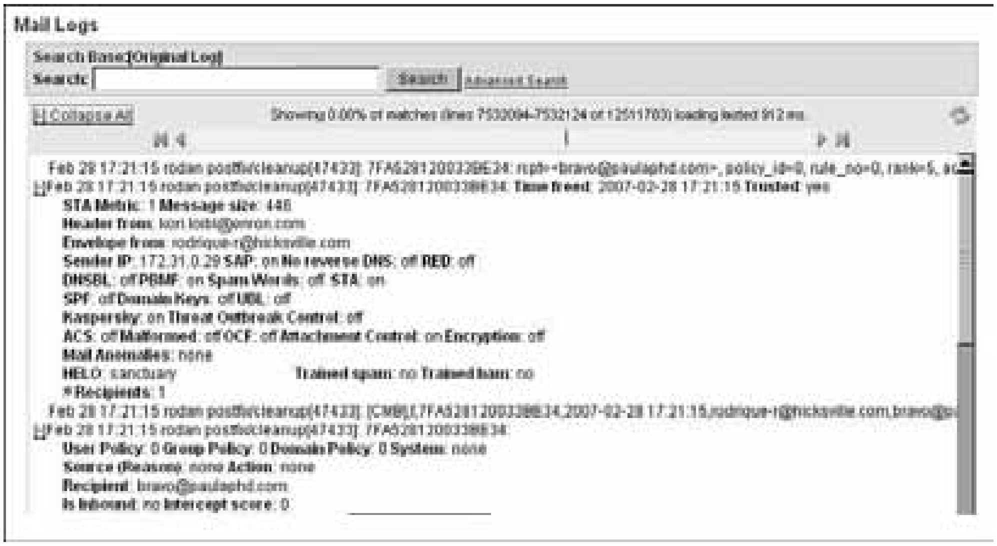


```
Showing 0.00% of matches (lines 7532094-7532124 of 12511703) loading lasted 912 ms.

   Feb 28 17:21:15 rodan postfix/cleanup[47433]: 7FA528120033BE34: rcpt=<bravo@paulaphd.com>, policy_id=0, rule_no=0, rank=5, ac
[+]Feb 28 17:21:15 rodan postfix/cleanup[47433]: 7FA528120033BE34: [RM01],smtp,2007-02-28 17:21:15,2007-02-28 17:21:15,%2c173
   Feb 28 17:21:15 rodan postfix/cleanup[47433]: [CMB],[,7FA528120033BE34,2007-02-28 17:21:15,rodrique-r@hicksville.com,bravo@pa
[+]Feb 28 17:21:15 rodan postfix/cleanup[47433]: 7FA528120033BE34: [RR01],2007-02-28 17:21:15,0,0,0,--,--,--,,bravo@paulaphd.cor
   Feb 28 17:21:15 rodan postfix/qmgr[09534]: 7FA528120033BE34: from=<rodrique-r@hicksville.com>, size=446, nrcpt=2 (queue active
   Feb 28 17:21:15 rodan postfix/cleanup[49414]: 4ABC1B100C11F7BE: message-id=<fed3.0003.00000001@outland.borderware.com
   Feb 28 17:21:15 rodan postfix/smtpd[42064]: CC: [RC01],2007-02-28 17:21:15,unknown,172.31.0.29,,,,,--,--,"
   Feb 28 17:21:15 rodan postfix/smtpd[42064]: disconnect from unknown[172.31.0.29]
   Feb 28 17:21:15 rodan postfix/smtpd[43274]: connect from unknown[172.31.0.29]
   Feb 28 17:21:15 rodan postfix/smtpd[43274]: connect from unknown[172.31.0.29]
   Feb 28 17:21:15 rodan postfix/smtp[45425]: 7FA528120033BE34: to=<bravo@paulaphd.com>, relay=172.20.25.4[172.20.25.4], delay=
[+]Feb 28 17:21:15 rodan postfix/smtp[45425]: 7FA528120033BE34: [RR01],2007-02-28 17:21:15,"","","",mta,--,snt,bravo@paulaphd.cor
   Feb 28 17:21:15 rodan postfix/cleanup[49432]: FF3409020C034D1C: entry_time=1172701275.912859
   Feb 28 17:21:15 rodan postfix/smtpd[43274]: FF3409020C034D1C: client=unknown[172.31.0.29]
   Feb 28 17:21:15 rodan postfix/cleanup[49432]: FF3409020C034D1C: message-id=<17312.0003.00000001@sanctuary.borderware.co
   Feb 28 17:21:15 rodan postfix/cleanup[49414]: 4ABC1B100C11F7BE: rcpt=<griffith-i@hicksville.com>, policy_id=0, rule_no=0, rank=5,
[+]Feb 28 17:21:15 rodan postfix/cleanup[49414]: 4ABC1B100C11F7BE: [RM01],smtp,2007-02-28 17:21:15,2007-02-28 17:21:15,%3c6e
   Feb 28 17:21:15 rodan postfix/cleanup[49414]: [CMB],[,4ABC1B100C11F7BE,2007-02-28 17:21:15,foxtrot@circlecityconvetteclub.org,gri
```

The start of a single message log entry begins with a connect message, and ends with the disconnect message. To make sure that you are looking at the entries for a specific message, check the message ID
(for example, 7FA528120033BE34) for each log entry.

3. Click **Expand All** to show a summary of the processing for the message.



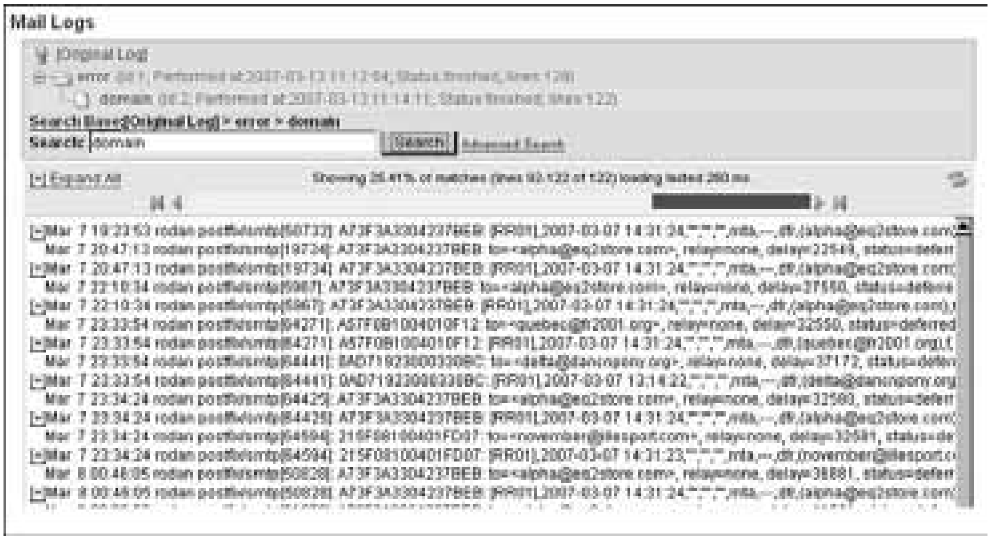
```
Showing 0.00% of matches (lines 7532094-7532124 of 12511703) loading lasted 912 ms.

   Feb 28 17:21:15 rodan postfix/cleanup[47433]: 7FA528120033BE34: rcpt=<bravo@paulaphd.com>, policy_id=0, rule_no=0, rank=5, ac
[-]Feb 28 17:21:15 rodan postfix/cleanup[47433]: 7FA528120033BE34: Time fixed: 2007-02-28 17:21:15 Trusted: yes
      STA Metric: 1 Message size: 446
      Header from: kori.lobb@enron.com
      Envelope from: rodrique-r@hicksville.com
      Sender IP: 172.31.0.29 SAP: on No reverse DNS: off RED: off
      DNSBL: off PBMF: on Spam Words: off STA: on
      SPF: off Domain Keys: off UBL: off
      Kaspersky: on Threat Outbreak Control: off
      ACS: off Malformed: off OCF: off Attachment Control: on Encryption: off
      Mail Anomalies: none
      HELO: sanctuary                    Trained spam: no Trained ham: no
      #Recipients: 1
   Feb 28 17:21:15 rodan postfix/cleanup[47433]: [CMB],[,7FA528120033BE34,2007-02-28 17:21:15,rodrique-r@hicksville.com,bravo@pa
[-]Feb 28 17:21:15 rodan postfix/cleanup[47433]: 7FA528120033BE34:
      User Policy: 0 Group Policy: 0 Domain Policy: 0 System: none
      Source (Reason): none Action: none
      Recipient: bravo@paulaphd.com
      Is Inbound: no Intercept score: 0
```

Search the Mail Log

To search the mail log:

1. In the **Search** text box, type a text string to search for.
2. Click **Search**.
   You can add multiple searches to the original search to further filter the results.
3. Click the **Remove** button to remove the previous search base, or click **Search Base (Original Log)** to start a new search.

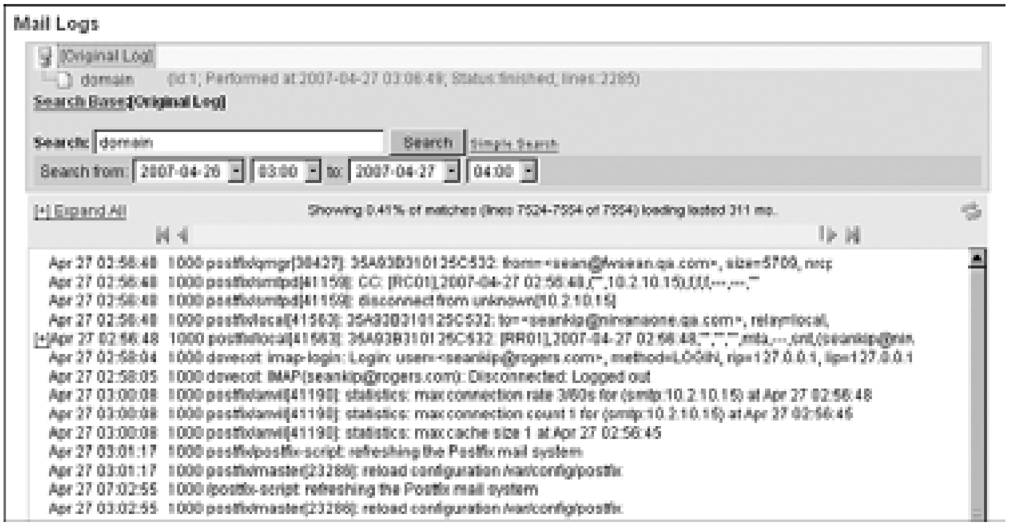


error (id:1, Performed at:2007-03-13 11:12:54; Status:finished; lines:128)
domain (id:2, Performed at:2007-03-13 11:14:11; Status:finished; lines:122)
Search Base[Original Log] > error > domain
Search: domain
Showing 25.41% of matches (lines 93-122 of 122) loading lasted 260 ms.

```
[+]Mar  7 19:23:53 rodan postfix/smtp[50733]: A73F3A3304237BEB: [RR01],2007-03-07 14:31:24,"","","",mta,--,dlt,(alpha@eq2store.com(
   Mar  7 20:47:13 rodan postfix/smtp[19734]: A73F3A3304237BEB: to=<alpha@eq2store.com>, relay=none, delay=22549, status=deferr
[+]Mar  7 20:47:13 rodan postfix/smtp[19734]: A73F3A3304237BEB: [RR01],2007-03-07 14:31:24,"","","",mta,--,dlt,(alpha@eq2store.com(
   Mar  7 22:10:34 rodan postfix/smtp[5967]: A73F3A3304237BEB: to=<alpha@eq2store.com>, relay=none, delay=27550, status=deferre
[+]Mar  7 22:10:34 rodan postfix/smtp[5967]: A73F3A3304237BEB: [RR01],2007-03-07 14:31:24,"","","",mta,--,dlt,(alpha@eq2store.com),(
   Mar  7 23:33:54 rodan postfix/smtp[64271]: A57F0B1004010F12: to=<quebec@fr2001.org>, relay=none, delay=32550, status=deferred
[+]Mar  7 23:33:54 rodan postfix/smtp[64271]: A57F0B1004010F12: [RR01],2007-03-07 14:31:24,"","","",mta,--,dlt,(quebec@fr2001.org),(
   Mar  7 23:33:54 rodan postfix/smtp[64441]: 0AD719230D0330BC: to=<delta@dancingpony.org>, relay=none, delay=37172, status=deferr
[+]Mar  7 23:33:54 rodan postfix/smtp[64441]: 0AD719230D0330BC: [RR01],2007-03-07 13:14:22,"","","",mta,--,dlt,(delta@dancingpony.org
   Mar  7 23:34:24 rodan postfix/smtp[64425]: A73F3A3304237BEB: to=<alpha@eq2store.com>, relay=none, delay=32580, status=deferr
[+]Mar  7 23:34:24 rodan postfix/smtp[64425]: A73F3A3304237BEB: [RR01],2007-03-07 14:31:24,"","","",mta,--,dlt,(alpha@eq2store.com(
   Mar  7 23:34:24 rodan postfix/smtp[64594]: 215F08100401FD07: to=<november@ilesport.com>, relay=none, delay=32581, status=de
[+]Mar  7 23:34:24 rodan postfix/smtp[64594]: 215F08100401FD07: [RR01],2007-03-07 14:31:23,"","","",mta,--,dlt,(november@ilesport.c
   Mar  8 00:46:05 rodan postfix/smtp[50828]: A73F3A3304237BEB: to=<alpha@eq2store.com>, relay=none, delay=36881, status=deferr
[+]Mar  8 00:46:05 rodan postfix/smtp[50828]: A73F3A3304237BEB: [RR01],2007-03-07 14:31:24,"","","",mta,--,dlt,(alpha@eq2store.com(
```

By default, the search only applies to the last 24 hours of logs.

4. Click **Advanced Search** to modify the specific time period for the search.



domain (id:1; Performed at:2007-04-27 03:06:49; Status:finished; lines:2285)
Search Base[Original Log]
Search: domain
Search from: 2007-04-26 03:00 to: 2007-04-27 04:00
Showing 0.41% of matches (lines 7524-7554 of 7554) loading lasted 311 ms.

```
   Apr 27 02:56:48  1000 postfix/qmgr[38427]: 35A93B310125C532: from=<sean@fwsean.qa.com>, size=5709, nrcp
   Apr 27 02:56:48  1000 postfix/smtpd[41159]: CC: [RC01],2007-04-27 02:56:48,("",10.2.10.15),(),(--,--,"
   Apr 27 02:56:48  1000 postfix/smtpd[41159]: disconnect from unknown[10.2.10.15]
   Apr 27 02:56:48  1000 postfix/local[41563]: 35A93B310125C532: to=<seankip@nirvanaone.qa.com>, relay=local,
[+]Apr 27 02:56:48  1000 postfix/local[41563]: 35A93B310125C532: [RR01],2007-04-27 02:56:48,"","","",mta,--,cnt,(seankip@nirv
   Apr 27 02:58:04  1000 dovecot: imap-login: Login: user=<seankip@rogers.com>, method=LOGIN, rip=127.0.0.1, lip=127.0.0.1
   Apr 27 02:58:05  1000 dovecot: IMAP(seankip@rogers.com): Disconnected: Logged out
   Apr 27 03:00:08  1000 postfix/anvil[41190]: statistics: max connection rate 3/60s for (smtp:10.2.10.15) at Apr 27 02:56:48
   Apr 27 03:00:08  1000 postfix/anvil[41190]: statistics: max connection count 1 for (smtp:10.2.10.15) at Apr 27 02:56:45
   Apr 27 03:00:08  1000 postfix/anvil[41190]: statistics: max cache size 1 at Apr 27 02:56:45
   Apr 27 03:01:17  1000 postfix/postfix-script: refreshing the Postfix mail system
   Apr 27 03:01:17  1000 postfix/master[23286]: reload configuration /var/config/postfix
   Apr 27 07:02:55  1000 /postfix-script: refreshing the Postfix mail system
   Apr 27 03:02:55  1000 postfix/master[23286]: reload configuration /var/config/postfix
```

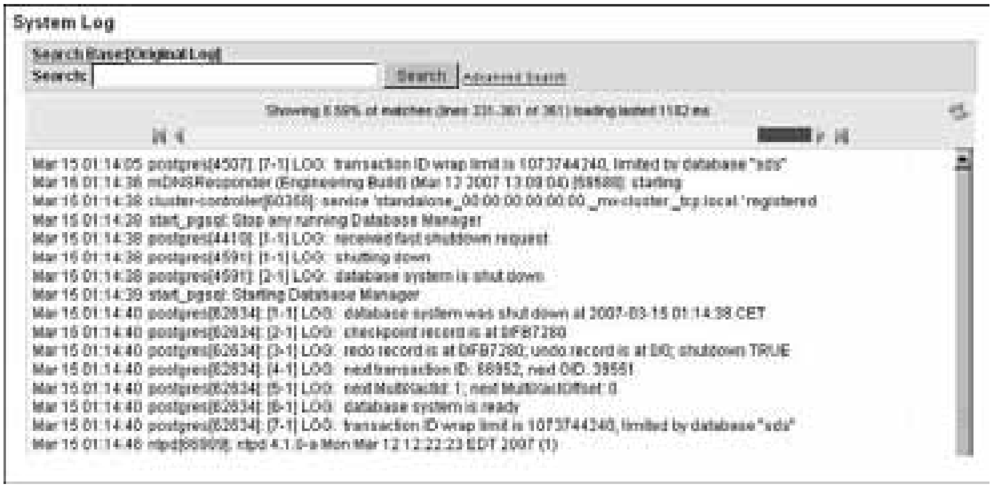
System Logs

The *System Log* contains all system-related messages, for example, file uploads, backup status, virus pattern file updates, Reputation Enabled Defense service connections, LDAP connection status, and other types of status messages.

To access the system log files:

1. Select **Activity > Logs > System**.
   The System Log page appears and displays the end of the log file.
2. Use the slider control to page through the log file, or use the right and left arrow icons.

   You can also jump to the start or end of the log file using the arrow icons as required.



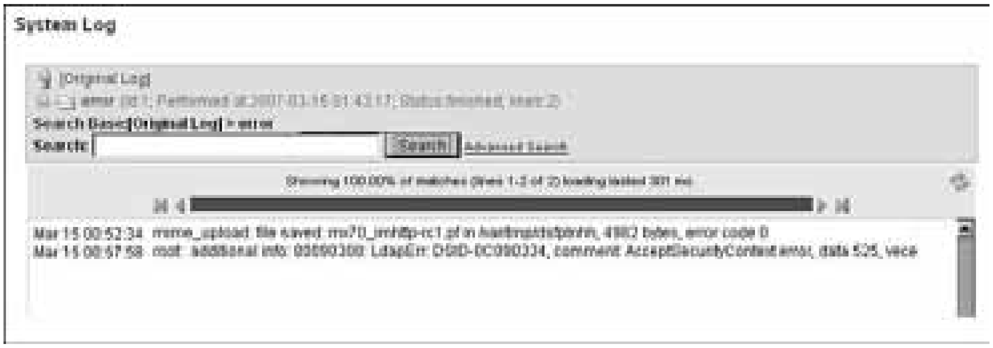
```
Showing 8.59% of matches (lines 331-361 of 361) loading lasted 1182 ms

Mar 15 01:14:05 postgres[4507]: [7-1] LOG:  transaction ID wrap limit is 1073744240, limited by database "sds"
Mar 15 01:14:36 mDNSResponder (Engineering Build) (Mar 12 2007 13:09:04) [59580]: starting
Mar 15 01:14:38 cluster-controller[60368]: service 'standalone_00:00:00:00:00:00._mx-cluster._tcp.local.' registered
Mar 15 01:14:29 start_pgsql: Stop any running Database Manager
Mar 15 01:14:38 postgres[4410]: [1-1] LOG:  received fast shutdown request
Mar 15 01:14:38 postgres[4591]: [1-1] LOG:  shutting down
Mar 15 01:14:38 postgres[4591]: [2-1] LOG:  database system is shut down
Mar 15 01:14:39 start_pgsql: Starting Database Manager
Mar 15 01:14:40 postgres[62834]: [1-1] LOG:  database system was shut down at 2007-03-15 01:14:38 CET
Mar 15 01:14:40 postgres[62834]: [2-1] LOG:  checkpoint record is at 0/FB7280
Mar 15 01:14:40 postgres[62834]: [3-1] LOG:  redo record is at 0/FB7280; undo record is at 0/0; shutdown TRUE
Mar 15 01:14:40 postgres[62834]: [4-1] LOG:  next transaction ID: 68952; next OID: 39561
Mar 15 01:14:40 postgres[62834]: [5-1] LOG:  next MultiXactId: 1; next MultiXactOffset: 0
Mar 15 01:14:40 postgres[62834]: [6-1] LOG:  database system is ready
Mar 15 01:14:40 postgres[62834]: [7-1] LOG:  transaction ID wrap limit is 1073744240, limited by database "sds"
Mar 15 01:14:46 ntpd[66909]: ntpd 4.1.0-a Mon Mar 12 12:22:23 EDT 2007 (1)
```

Search the System Log

To search the system log:

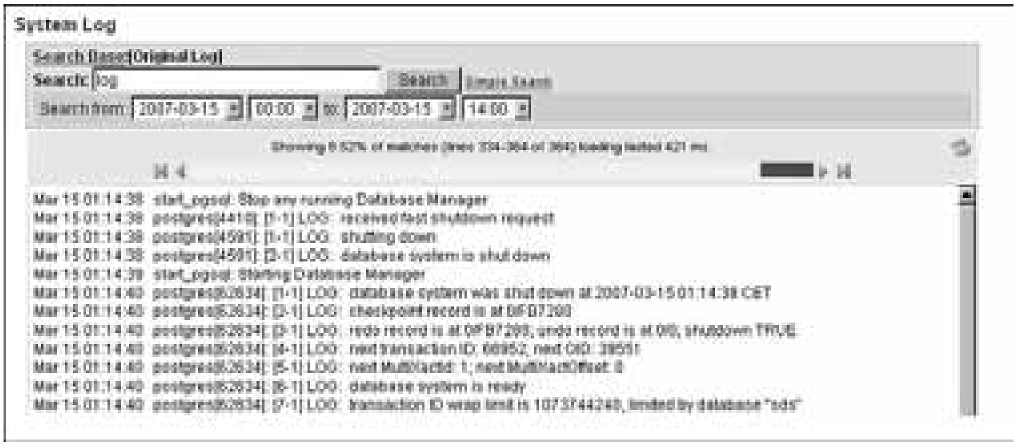
1. In the **Search** text box, type a text string to search for.
2. Click **Search**.
   You can add multiple searches to the original search to further filter the results.


System Log
[Original Log]
error (id 1; Performed at 2007-03-15 01:43:17; Status finished; lines 2)
Search Base[Original Log] > error
Search:
Search
Advanced Search

```
Showing 100.00% of matches (lines 1-2 of 2) loading lasted 301 ms

Mar 15 00:52:34  mime_upload: file saved: mx70_imhttp-rc1.pf in /var/tmp/cds/pbnhh, 4982 bytes, error code 0
Mar 15 00:57:58  mod:  additional info: 00090308: LdapErr: DSID-0C090334, comment: AcceptSecurityContext error, data 525, vece
```

3. Click the **Remove** button to remove the previous search base, or click **Search Base (Original Log)** to start a new search again.
   By default the search only applies to the last 24 hours of logs.
4. Click **Advanced Search** to modify the specific time period for the search.

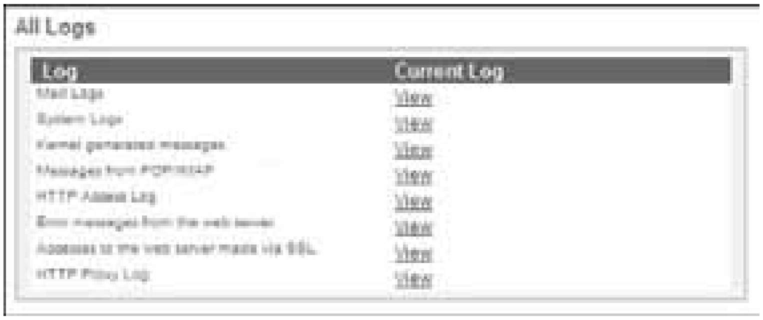

System Log
Search Base: [Original Log]
Search: log
Search
Simple Search
Search from: 2007-03-15 00:00 to: 2007-03-15 14:00

Showing 8.52% of matches (lines 334-364 of 364) loading lasted 421 ms

```
Mar 15 01:14:38  start_pgsql: Stop any running Database Manager
Mar 15 01:14:38  postgres[4410]: [1-1] LOG:  received fast shutdown request
Mar 15 01:14:38  postgres[4591]: [1-1] LOG:  shutting down
Mar 15 01:14:38  postgres[4591]: [2-1] LOG:  database system is shut down
Mar 15 01:14:39  start_pgsql: Starting Database Manager
Mar 15 01:14:40  postgres[62634]: [1-1] LOG:  database system was shut down at 2007-03-15 01:14:38 CET
Mar 15 01:14:40  postgres[62634]: [2-1] LOG:  checkpoint record is at 0/FB7280
Mar 15 01:14:40  postgres[62634]: [3-1] LOG:  redo record is at 0/FB7280; undo record is at 0/0; shutdown TRUE
Mar 15 01:14:40  postgres[62634]: [4-1] LOG:  next transaction ID: 66952; next OID: 28561
Mar 15 01:14:40  postgres[62634]: [5-1] LOG:  next MultiXactId: 1; next MultiXactOffset: 0
Mar 15 01:14:40  postgres[62634]: [6-1] LOG:  database system is ready
Mar 15 01:14:40  postgres[62634]: [7-1] LOG:  transaction ID wrap limit is 1073744240, limited by database "sds"
```

WatchGuard XCS Logs

Select **Activity > Logs > All Logs** to access all system log files.


All Logs

Log	Current Log
Mail Logs	View
System Logs	View
Kernel generated messages	View
Messages from POP/IMAP	View
HTTP Access Log	View
Error messages from the web server	View
Accesses to the web server made via SSL	View
HTTP Proxy Log	View

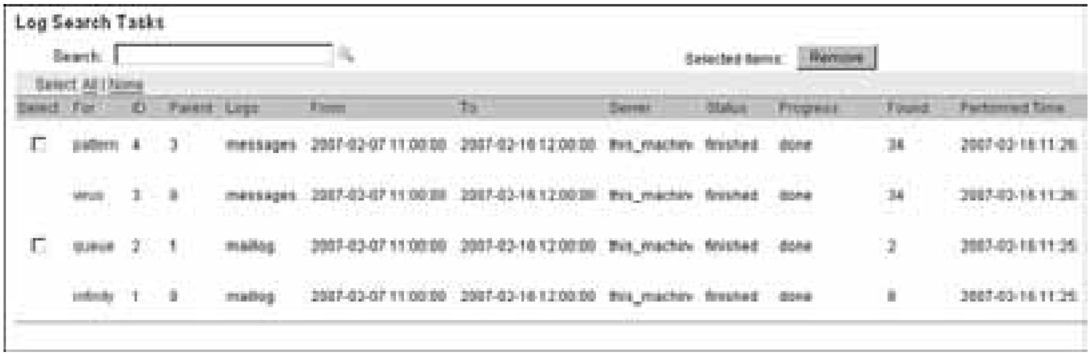
- **Mail Logs** – A log of all mail processing activity.
- **System Logs** – A log of all system-related messages. This includes LDAP imports, backup and restore, Anti-virus updates, and others.
- **Kernel Generated Messages** – A log from the system kernel.
- **Messages From POP/IMAP Logins** – Contains messages from POP, IMAP, and WebMail logins. This includes admin and console logins.
- **HTTP Access Log** – A log of HTTPS access to the web server.
- **Error Messages From the Web Server** – Contains error messages from the internal web server.
- **Accesses to the Web Server Made Via SSL** – A log of SSL web server access. This log displays accessed web pages and the connecting IP address.
- **HTTP Proxy Log** – Contains messages generated by the Web Proxy.

Previous Searches

To see a list of previous log searches that have been performed on the system:

1. Select **Activity > Logs > Previous Searches**.
   The Log Search Tasks page appears.
2. In the list of previous searches, click on a specific search to apply the search query to the most recent data in the logs and view the results.
   This allows you to save your favorite types of searches.

3. In the **Search** text box, type a text string and click the search icon to filter the search results.
4. To delete specific searches, select the corresponding check box, and then click **Remove**.



Log Search Tasks

Search: [ ] Selected items: Remove

Select All | None

Select	For	ID	Parent	Logs	From	To	Server	Status	Progress	Found	Performed Time
☐	pattern	4	3	messages	2007-02-07 11:00:00	2007-02-16 12:00:00	this_machin	finished	done	34	2007-02-16 11:26
	virus	3	0	messages	2007-03-07 11:00:00	2007-03-16 12:00:00	this_machin	finished	done	34	2007-03-16 11:26
☐	queue	2	1	maillog	2007-03-07 11:00:00	2007-03-16 12:00:00	this_machin	finished	done	2	2007-03-16 11:25
	infinity	1	0	maillog	2007-03-07 11:00:00	2007-03-16 12:00:00	this_machin	finished	done	8	2007-03-16 11:25

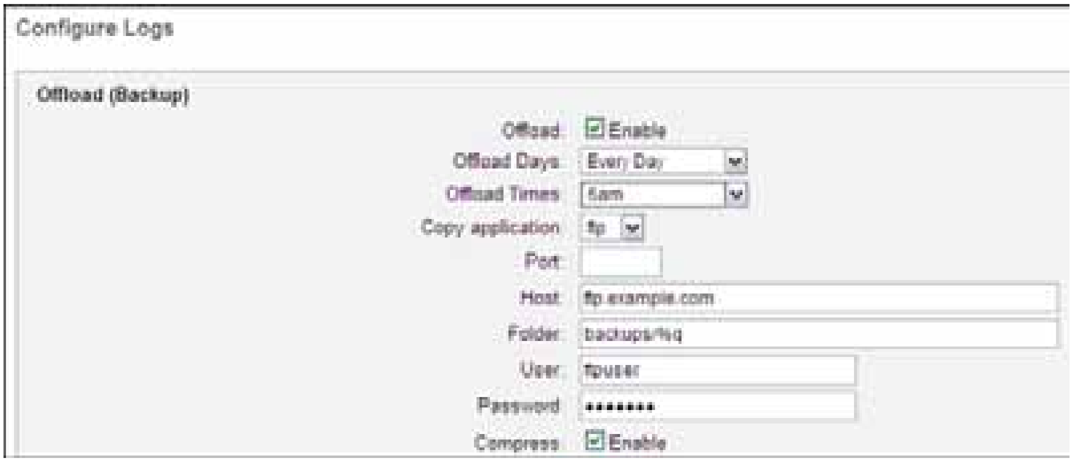
Configure Logs

For backup purposes and offline reporting, the WatchGuard XCS can copy log and reporting files to another system at regular intervals using FTP or SCP file copy utilities. This allows you to backup the log files to a separate host for analysis and storage. When you enable this option, the offload occurs each time a log file is rolled over and for the time period specified in the offload date and time. Logs are saved with a timestamp, for example, “maillog.200901010000”.

> ***Note*** *The Offload (Reporting) section is used for organizations that require a separate reporting server to which logs are forwarded.*

To configure your rollout and offload settings (Backup and Offload):

1. Select **Configuration > Miscellaneous > Logs**.
   The Configure Logs page appears.



Configure Logs

Offload (Backup)

Offload: ☑ Enable
Offload Days: Every Day
Offload Times: 6am
Copy application: ftp
Port:
Host: ftp.example.com
Folder: backups/%q
User: ftpuser
Password: •••••••
Compress: ☑ Enable

2. To enable the offload of rollout log files, select the **Offload** check box.
3. From the **Offload Days** drop-down list, select the days on which to offload log files.
4. From the **Offload Times** drop-down list, select the time to offload log files.
5. From the **Copy application** drop-down list, select whether to use **FTP** or **SCP** for copy rollout files.
   You must enable these applications on the destination host.

> ***Note*** *When you set up an SCP server, make sure you disable PAM authentication and enable the built-in authentication. If the WatchGuard XCS is behind a network firewall, you must open up TCP port 22 to your SCP server.*

6. In the **Port** text box, type the TCP port used by the copy application (FTP or SCP).
   If this field is left blank, default port values (FTP: port 21, SCP: port 22) are assumed.
7. In the **Host** text box, type the host to which the rollout data is copied to using the specified method.

   For example, ftp.example.com.

8. In the **Folder** text box, type the folder to which the rollout data is copied to.

   For clustered systems, use %q to add the name of the clustered system to the folder name.
   For example, `backups/%q`.

9. In the **User** text box, type a user name to log in to the destination host.
10. In the **Password** text box, type a password for the user.
11. To enable gzip compression of the rollout file, select the **Compress** check box.
12. Click **Update** when finished.
13. Click **Offload now** to begin the offload of the files immediately.

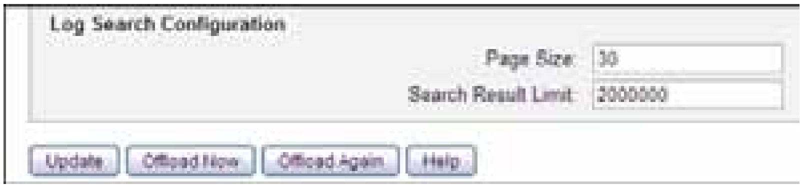
    Click the **Offload Again** button to reset the information of offloaded files.

    This action forces an offload of all files (even those offloaded before) again. You must click **Offload Now**, or wait for the next scheduled offload (when a log file has rolled over, or every hour) to start the offloading process after you click **Offload Again**.

> ***Note*** *Logs are not removed from the device when they are offloaded.*

Log Search Configuration

These options configure the defaults settings for all log searches:


Log Search Configuration

Page Size: 30

Search Result Limit: 2000000

Page Size

Type the amount of entries in a log file to show on one search page. The default value is 30.

Search Result Limit

Type the default number of entries returned from a search. The default value is 200000.

20 System Management

Backup

The WatchGuard XCS can back up all data. This includes the reporting database, quarantined items, mail queues, user mail directories, uploaded user lists, SSL certificates, feature keys, and the system configuration.

The XCS supports three backup methods:

- FTP server (recommended for large, full backups)
- SCP (Secure Copy) server
- Local disk (for small size or partial configuration backups downloaded to a workstation)

Warning *We strongly recommended that you use the FTP backup method for large backup requirements. You must use Local Disk backups for only small, partial configuration backups. The XCS device cannot restore a local backup file over 2GB in size.*

Restore from Backup

The restore feature can restore any of the backup items individually. The XCS device must be backed up before performing any type of software upgrade or update. The restore operation restores the configuration and reporting data in two separate stages.

- **Configuration restore** – The XCS configuration is restored first. This process takes only a short amount of time and you can quickly return to the administrative user interface to start processing messages again. A critical alarm “Critical Restore: Complete PASSED” is generated to alert you when this first stage of the restore is complete.
- **Reporting data restore** – The reporting data (if required) is then restored as a background process. This process is performed while the system is processing messages. When restoring reporting data, it may take 24 to 72 hours before the restore is fully completed, depending on the amount of data that is restored. These serious alarms are generated at different points in the reporting restore process:

- ○ "Serious: RESTORE: Reporting: Recovery Started": This indicates that the online reporting restore process has started and data is copying into a temporary database.
- ○ "Serious: RESTORE: Reporting: Migration Started": This indicates the data has been fully copied into the temporary database and migrating to the online database.
- ○ "Serious: RESTORE: Reporting: Recovery Complete": This indicates that the online reporting restore process is complete.

Message processing performance is negatively affected when restoring reporting data to an XCS device that is currently processing messages. If you reboot the system during the reporting restore process, the process continues when the system restarts.

> ***Note*** *In certain cases, large backup files cause the Backup page to time out and the "Backup Complete" button does not appear. You can still monitor the Backup process in the logs and the alarms.*

The size of the reporting database or quarantined mail area can be very large. If reporting data and quarantined mail are not required, we recommend that you do not back up this data to provide a manageable backup file size.

> ***Note*** *Restoring a clustered device requires a different procedure than outlined in the next section.*
> *See Cluster Management for more information on the backup and restore procedure for a cluster.*

Backup File Name

The naming convention for backup files is:

```
MG-BCKUP.YYMMDDHHMM
```

For example,

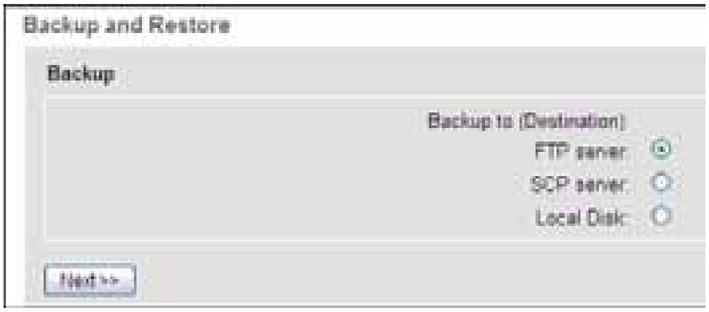
```
MG-BCKUP.1002152245
```

This indicates that the backup file is from Feb 15th, 2010 at 10:45PM. When you purge old backup files, make sure that you examine the timestamps before you delete them.

Start a Backup

To start a backup:

1. Select **Administration > Backup/Restore > Backup & Restore**.



Backup and Restore

Backup

Backup to (Destination)

FTP server ●

SCP server ○

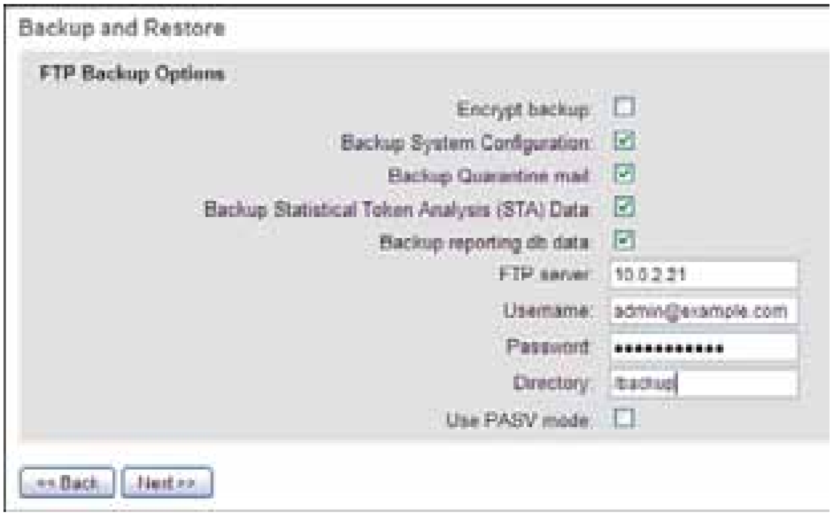
Local Disk ○

2. Select the backup destination and click **Next >>**.

FTP Backup Options

These options are available when you back up to an FTP server:

> **Note** *When you configure an FTP server, we recommend that you set the idle timeout value on the FTP server to a minimum of 1800 to 3600 seconds to make sure the connection does not timeout while the WatchGuard XCS performs the backup or restore process.*



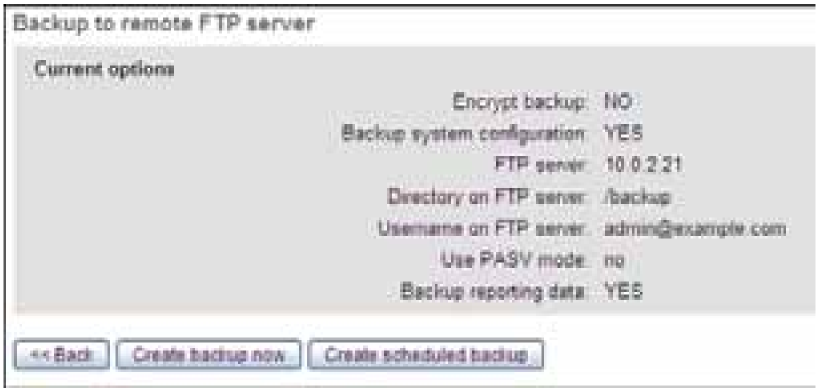
Backup and Restore

FTP Backup Options

Encrypt backup: □
Backup System Configuration: ☑
Backup Quarantine mail: ☑
Backup Statistical Token Analysis (STA) Data: ☑
Backup reporting db data: ☑
FTP server: 10.0.2.21
Username: admin@example.com
Password: ••••••••••••
Directory: /backup
Use PASV mode: □

- **Encrypt Backup** – Encrypts the backup file to protect its contents.
- **Backup System Configuration** – Back up all configuration data. This includes mailboxes, licenses, and feature keys. You must enable this option if you need to restore system functionality.
- **Backup Quarantine Mail** – Back up all quarantined mail. Backing up quarantined mail may greatly increase the size of the backup file.
- **Backup Token Analysis Data** – Back up the Token Analysis database.
- **Backup Reporting Data** – Back up the entire reporting database. This greatly increases the size of the backup file.
- **FTP server** – Type the host name or IP address of the destination FTP server.
- **Username** – Type the username for the FTP server.
- **Password** – Type the password for the FTP server.
- **Directory** – Type the directory path where the backup files are located on the FTP server.
- **Use PASV mode** – Set FTP to use passive mode if you experience problems when you connect to the FTP server.

When you have set your options, click **Next >>** to continue.



Backup to remote FTP server

Current options

Encrypt backup: NO

Backup system configuration: YES

FTP server: 10.0.2.21

Directory on FTP server: /backup

Username on FTP server: admin@example.com

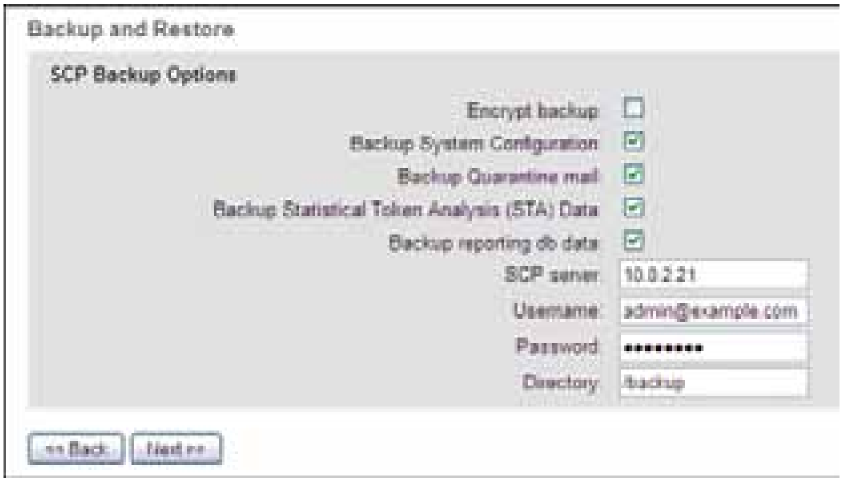
Use PASV mode: no

Backup reporting data: YES

Verify that your options are correct, and then click **Create backup now** to start the backup.
You can also click **Create scheduled backup** that takes you to the **Daily Backup** menu to create a scheduled FTP backup.

SCP Backup Options

These options are available when you back up to an SCP (Secure Copy) server:



Backup and Restore

SCP Backup Options

Encrypt backup: □

Backup System Configuration: ☑

Backup Quarantine mail: ☑

Backup Statistical Token Analysis (STA) Data: ☑

Backup reporting db data: ☑

SCP server: 10.0.2.21

Username: admin@example.com

Password: ••••••••••

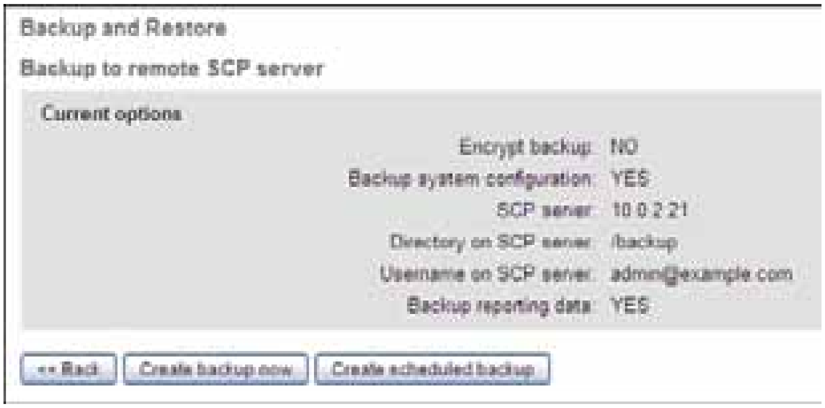
Directory: /backup

- **Encrypt Backup** – Encrypts the backup file to protect its contents.
- **Backup System Configuration** – Back up all configuration data. This includes mailboxes, licenses, and feature keys. You must enable this option if you need to restore system functionality.
- **Backup Quarantine Mail** – Back up all quarantined mail. Backing up quarantined mail may greatly increase the size of the backup file.
- **Backup Token Analysis Data** – Back up the Token Analysis database.
- **Backup Reporting Data** – Back up the entire reporting database. This greatly increases the size of the backup file.
- **SCP server** – Type the host name or IP address of the destination SCP server.

> ***Note*** *When you setup the SCP server, make sure that you disable PAM authentication and enable the built-in authentication. If the WatchGuard XCS is behind a network firewall, you must open TCP port 22 to your SCP server.*

- **Username** – Type the username for the SCP server.
- **Password**– Type the password for the SCP server.
- **Directory**– Type the directory path where the backup files are located on the SCP server.

When you have set your options, click **Next >>** to continue.



Backup and Restore

Backup to remote SCP server

Current options

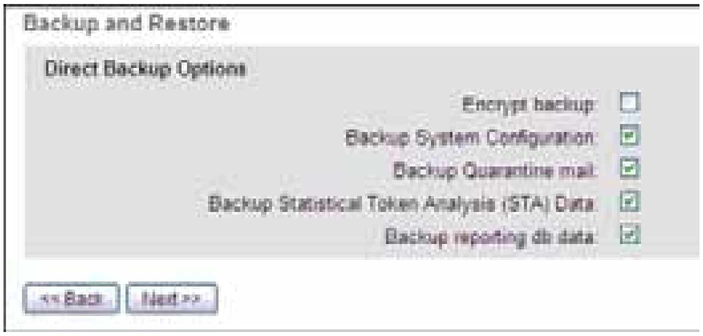
Encrypt backup:	NO
Backup system configuration:	YES
SCP server:	10.0.2.21
Directory on SCP server:	/backup
Username on SCP server:	admin@example.com
Backup reporting data:	YES

Verify that your options are correct, and then click **Create backup now** to start the backup.
You can also click **Create scheduled backup** that takes you to the **Daily Backup** menu to create a scheduled SCP backup.

Local Disk Options

These options are available when you back up to a local disk:

> ***Warning*** *It is strongly recommended that the FTP backup method be used for large backup requirements. Local Disk backups must only be used for small, partial configuration backups. The system cannot restore a local backup file over 2GB in size.*



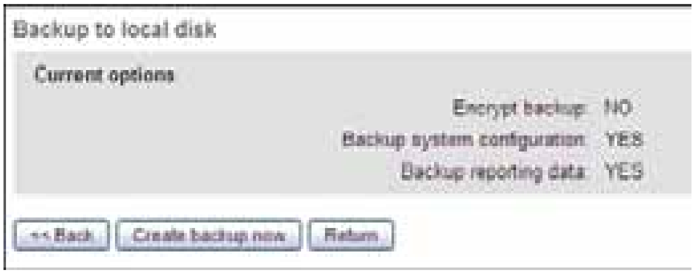
Backup and Restore

Direct Backup Options

Encrypt backup:	☐
Backup System Configuration:	☑
Backup Quarantine mail:	☑
Backup Statistical Token Analysis (STA) Data:	☑
Backup reporting db data:	☑

- **Encrypt Backup** – Encrypts the backup file to protect its contents.
- **Backup System Configuration** – Back up all configuration data. This includes mailboxes, licenses, and feature keys. You must enable this option if you need to restore system functionality.
- **Backup Quarantine Mail** – Back up all quarantined mail. Backing up quarantined mail may greatly increase the size of the backup file.
- **Backup Token Analysis Data** – Back up the Token Analysis database.
- **Backup Reporting Data** – Back up the entire reporting database. This greatly increases the size of the backup file. We recommend that you use the FTP or SCP method for very large backup files.

When you have set your options, click **Next >>** to continue.



Backup to local disk

Current options

Encrypt backup: NO
Backup system configuration: YES
Backup reporting data: YES

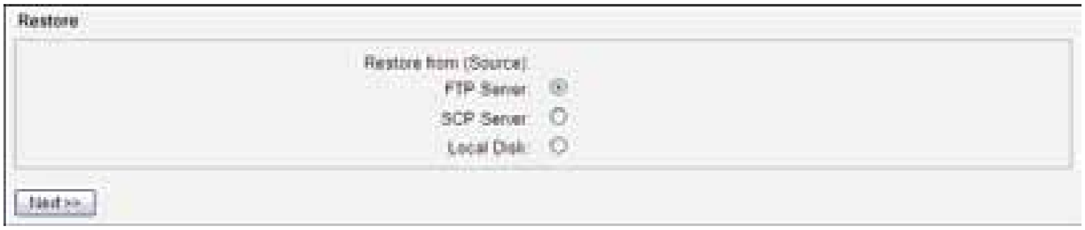
Verify that your options are correct, and then click **Create backup now** to start the backup.
You are prompted for a location to download the backup file (backup.gz). The backup file is saved in a gzip compressed archive.

Restore

Restore from backup

To start a restore:

1. Select **Administration > Backup/Restore > Backup & Restore**.



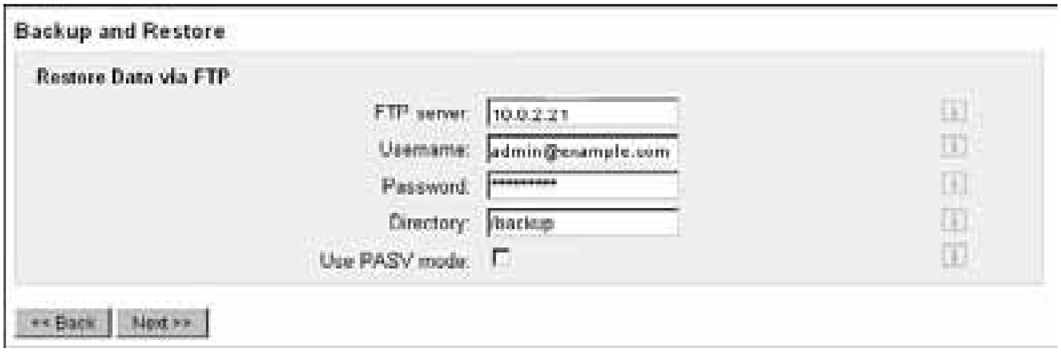
Restore

Restore from (Source):
FTP Server: ●
SCP Server: ○
Local Disk: ○

2. Select the restore method, and then click **Next >>**.

FTP Restore Options

Enter this information to restore from an FTP server:



Backup and Restore

Restore Data via FTP

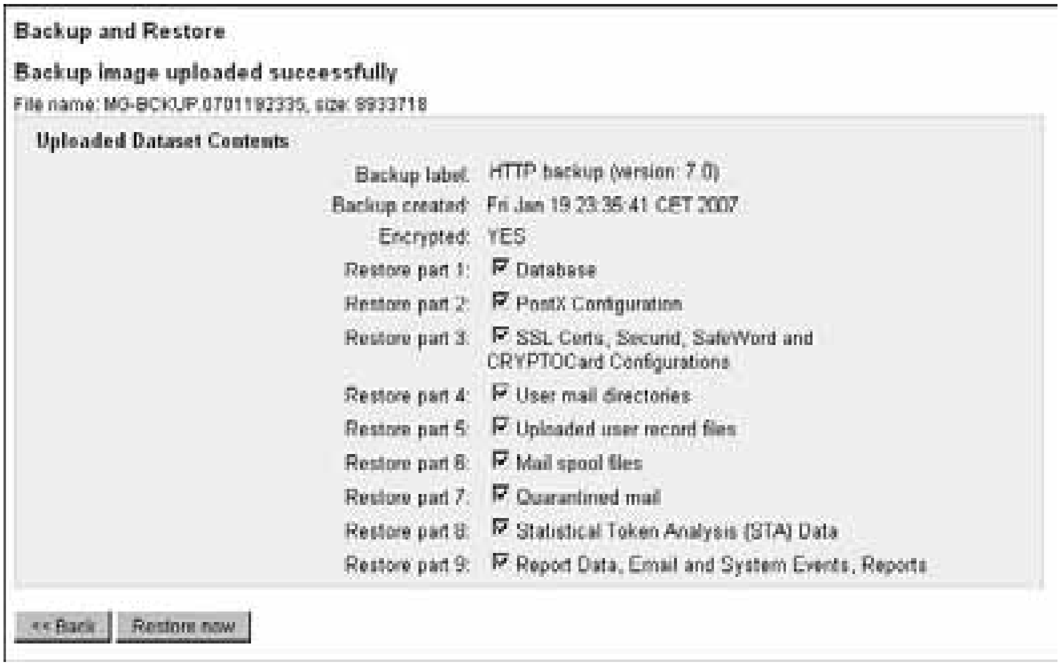
FTP server: 10.0.2.21
Username: admin@example.com
Password: **********
Directory: /backup
Use PASV mode: □

- **FTP server** – Type the host name or IP address of the FTP server where the backup file is stored.
- **Username** – Type the user name for the FTP server.
- **Password** – Type the password for the FTP server.
- **Directory** – Type the directory path where the backup files are located on the FTP server.

- **Use PASV mode** – Set FTP to use passive mode if you experience problems when you connect to the FTP server.
- Click **Next >>** to connect with the FTP server and restore the backup file.

> **Note** *In certain cases, large backup files cause the backup page to time out and the "Backup Complete" button does not appear. You can still monitor the backup process in the logs and in alarms. A critical alarm appears when the configuration restore operation is complete. A serious alarm appears when the background reporting restore process completes.*

When you have successfully retrieved the backup file, you can choose which aspects of the XCS configuration to restore. When you have finished selecting the restore items, click **Restore Now**.



Backup and Restore

Backup image uploaded successfully

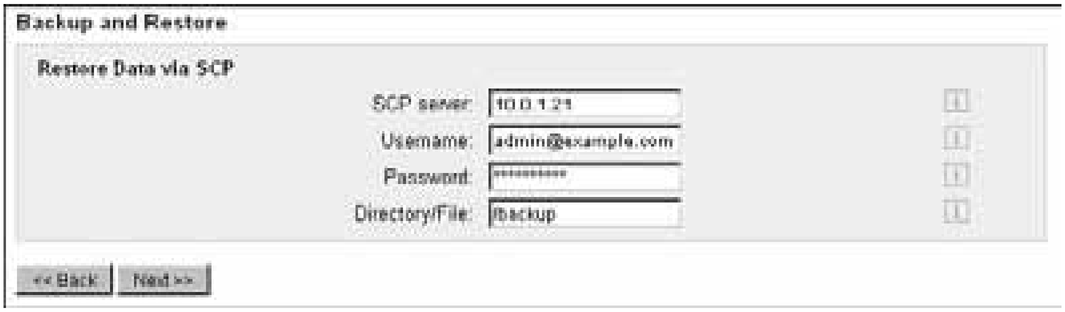
File name: MG-BCKUP.0701192335, size: 8933718

Uploaded Dataset Contents

Backup label: HTTP backup (version: 7.0)
Backup created: Fri Jan 19 23:35:41 CET 2007
Encrypted: YES
Restore part 1: ☑ Database
Restore part 2: ☑ PostX Configuration
Restore part 3: ☑ SSL Certs, Securid, SafeWord and CRYPTOCard Configurations
Restore part 4: ☑ User mail directories
Restore part 5: ☑ Uploaded user record files
Restore part 6: ☑ Mail spool files
Restore part 7: ☑ Quarantined mail
Restore part 8: ☑ Statistical Token Analysis (STA) Data
Restore part 9: ☑ Report Data, Email and System Events, Reports

Restore from SCP

Enter this information to restore from an SCP server:



Backup and Restore

Restore Data via SCP

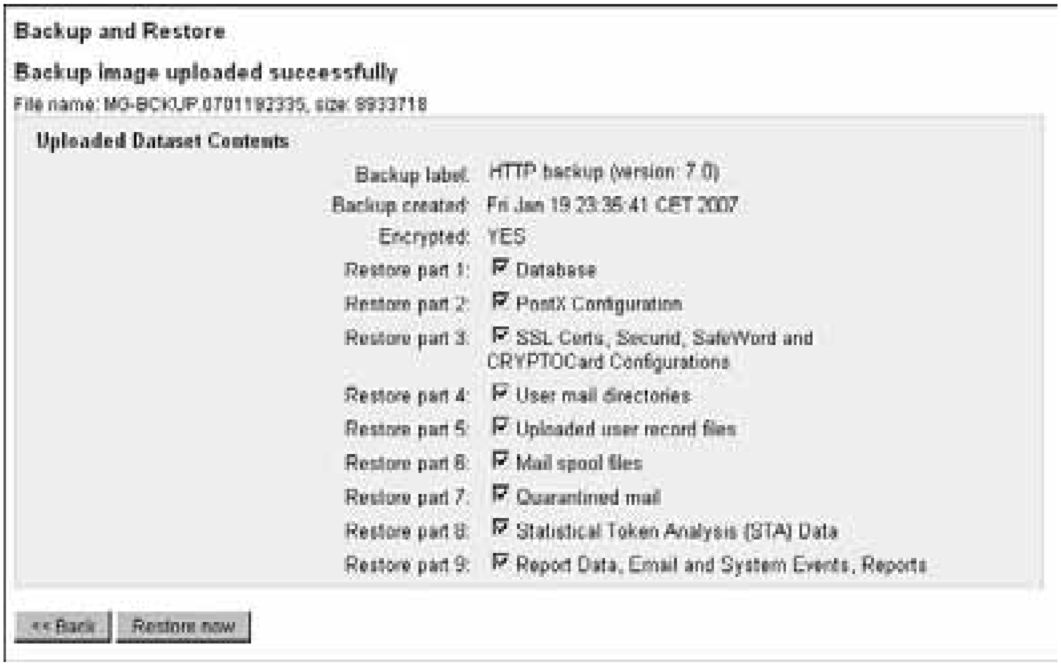
SCP server: 10.0.1.21
Username: admin@example.com
Password: **********
Directory/File: /backup

- **SCP server** – Type the host name or IP address of the SCP server.
- **Username** – Type the user name for the SCP server.

- **Password**– Type the password for the SCP server.
- **Directory**– Type the directory path where the backup file is located on the SCP server.
- Click **Next >>** to connect with the SCP server and restore the backup file.

> ***Note*** *In certain cases, large backup files cause the backup page to time out and the "Backup Complete" button does not appear. You can still monitor the backup process in the logs and in alarms. A critical alarm appears when the configuration restore operation is complete. A serious alarm appears when the background reporting restore process is complete.*

When you have successfully retrieved the backup file, you can choose which aspects of the XCS configuration to restore. When you have finished selecting the restore items, click **Restore Now**.



Backup and Restore

Backup image uploaded successfully

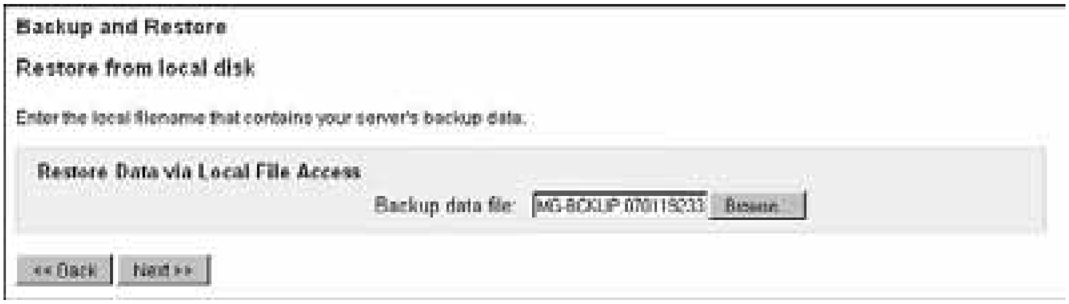
File name: MG-BCKUP.0701192335, size: 8933718

Uploaded Dataset Contents

Backup label: HTTP backup (version: 7.0)
Backup created: Fri Jan 19 23:35:41 CET 2007
Encrypted: YES
Restore part 1: ☑ Database
Restore part 2: ☑ PostX Configuration
Restore part 3: ☑ SSL Certs, Securid, SafeWord and CRYPTOCard Configurations
Restore part 4: ☑ User mail directories
Restore part 5: ☑ Uploaded user record files
Restore part 6: ☑ Mail spool files
Restore part 7: ☑ Quarantined mail
Restore part 8: ☑ Statistical Token Analysis (STA) Data
Restore part 9: ☑ Report Data, Email and System Events, Reports

Restore from Local Disk

Type the local filename that contains the backup file, or click **Browse** to select the file from the local drive directory listing. Click **Next >>** to upload and restore the backup file.



Backup and Restore

Restore from local disk

Enter the local filename that contains your server's backup data.

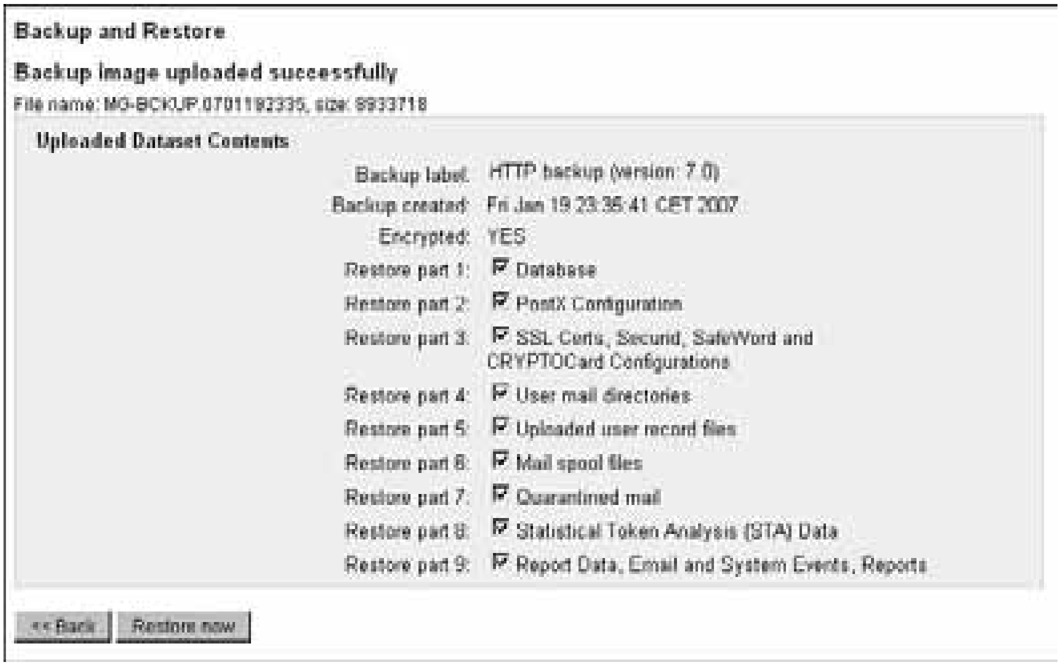
Restore Data via Local File Access

Backup data file: MG-BCKUP.070119233

Youcanviewthecurrentstatusoftherestoreprocessinthe**Status**sectionofthe**Administration>**
Backup/Restore>BackupandRestore
page.

> **Note** *In certain cases, large backup files cause the backup page to time out and the "Backup Complete" button does not appear. You can still monitor the backup process in the logs and in alarms. A critical alarm appears when the configuration restore operation is complete. A serious alarm appears when the background reporting restore process is complete.*

When you have successfully retrieved the backup file, you can choose which aspects of the XCS configuration to restore. When you have finished selecting the restore items, click **Restore Now**.



Backup and Restore

Backup image uploaded successfully

File name: MG-BCKUP.0701192335, size: 8933718

Uploaded Dataset Contents

Backup label: HTTP backup (version: 7.0)
Backup created: Fri Jan 19 23:35:41 CET 2007
Encrypted: YES
Restore part 1: ☑ Database
Restore part 2: ☑ PostX Configuration
Restore part 3: ☑ SSL Certs, Securid, SafeWord and CRYPTOCard Configurations
Restore part 4: ☑ User mail directories
Restore part 5: ☑ Uploaded user record files
Restore part 6: ☑ Mail spool files
Restore part 7: ☑ Quarantined mail
Restore part 8: ☑ Statistical Token Analysis (STA) Data
Restore part 9: ☑ Report Data, Email and System Events, Reports

When the restore is complete, review and edit your network configuration in the **Configuration > Network > Interfaces** page as required, and click **Apply** to reboot. This makes sure that all restored network settings are applied.

Backup and Restore Errors

This table describes the errors that can appear in the System Log when you restore a backup file:

Error Code	Description
0	No error
1	Form data missing
2	MIME data missing boundary
3	Invalid form data

Error Code	Description
4	Unsupported encoding method
5	Unsupported header in MIME data
6	File open error
7	Filename not specified
8	Error writing file
9	Data is incomplete

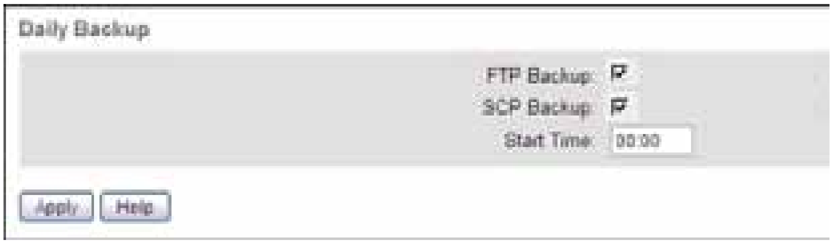
Daily Backup

You can schedule FTP and SCP backups to occur each day at a specific time. You must complete the FTP or SCP configuration first before you enable scheduled daily backups.

You can select **Activity > Logs > System** to view the results of daily backups.

To configure Daily Backups:

1. Select **Administration > Backup/Restore > Daily Backup**.



Daily Backup

FTP Backup: ☑

SCP Backup: ☑

Start Time: 00:00

2. Select the **FTP Backup** check box to use the FTP backup configuration for this scheduled backup.
3. Select the **SCP Backup** check box to use the SCP backup configuration for this scheduled backup.
4. In the **Start Time** text box, type the start time for the backup in 24-hour format HH:MM.

   For example, for 2:00AM, type `02:00`.

> ***Note*** *Because system reporting and log file maintenance starts at 00:00 midnight, we strongly recommend that you do not schedule daily backups between midnight and 1:00 AM.*

Add a Feature Key

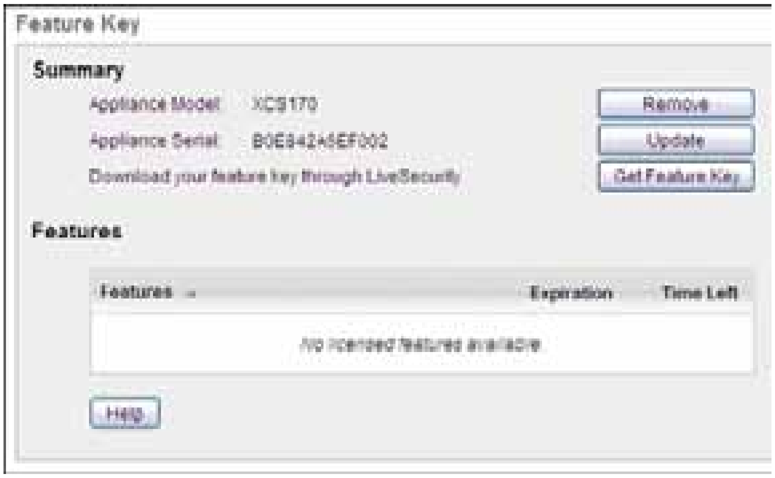
A feature key is a license that enables you to activate your purchased feature set on your WatchGuard XCS. You must register the device serial number on the WatchGuard LiveSecurity web site and retrieve your feature key before adding it to the WatchGuard XCS.

> ***Note*** *Make sure you can access the Internet if the device is installed behind a network firewall, or connects through an external proxy server.*

To install a new feature key:

1. Select **Administration > System > Feature Key**.

   The Feature Key page appears.



Feature Key

Summary

Appliance Model: XCS170

Appliance Serial: B0E84245EF002

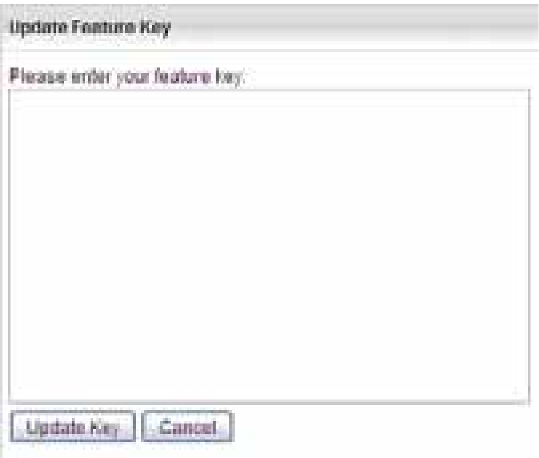
Download your feature key through LiveSecurity

Features

Features	Expiration	Time Left
No licensed features available		

2. Click **Update**.

   The Update Feature Key page appears.

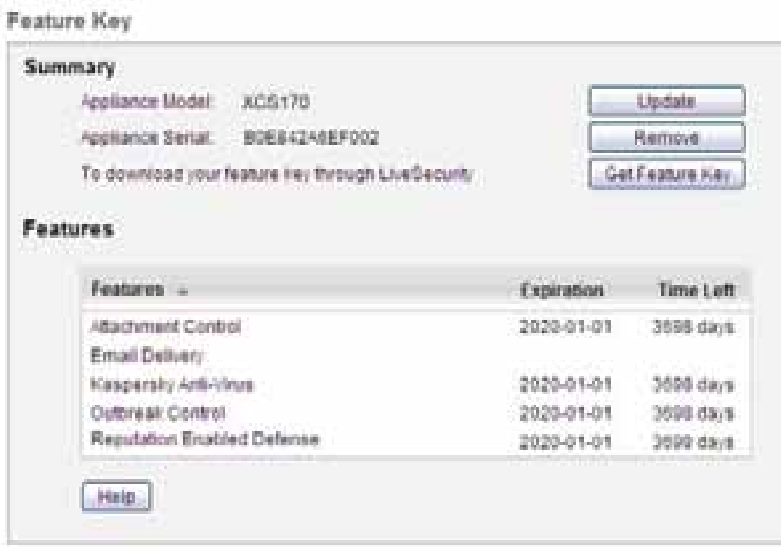


Update Feature Key

Please enter your feature key:

3. Copy the text of the feature key file and paste it in the text box.
4. Click **Update Key**.

   The Feature Key page appears with the new feature key information.



Feature Key

Summary

Appliance Model: XCS170

Appliance Serial: B0E84248EF002

To download your feature key through LiveSecurity

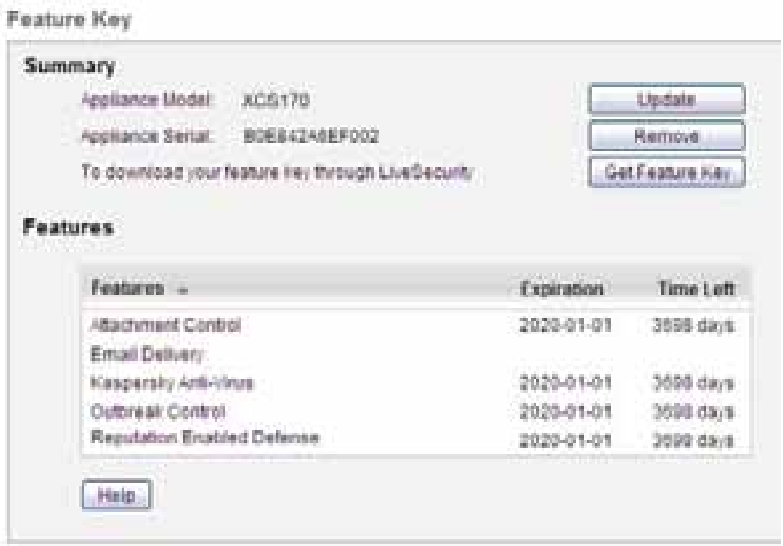
Features	Expiration	Time Left
Attachment Control	2020-01-01	3598 days
Email Delivery		
Kaspersky Anti-Virus	2020-01-01	3598 days
Outbreak Control	2020-01-01	3598 days
Reputation Enabled Defense	2020-01-01	3598 days

Update a Feature Key

If you already have a LiveSecurity login and your WatchGuard device serial number is registered, you can update your feature key automatically from the LiveSecurity site.

To update a feature key:

1. Select **Administration > System > Feature Key**.
   The Feature Key page appears.



Feature Key

Summary

Appliance Model: XCS170

Appliance Serial: B0E84248EF002

To download your feature key through LiveSecurity

Features	Expiration	Time Left
Attachment Control	2020-01-01	3598 days
Email Delivery		
Kaspersky Anti-Virus	2020-01-01	3598 days
Outbreak Control	2020-01-01	3598 days
Reputation Enabled Defense	2020-01-01	3598 days

2. Click **Get Feature Key**.
   Your feature key is downloaded from the LiveSecurity site and automatically updated on your device.

Troubleshoot Feature Key Updates

If you encounter errors when you add your feature key:

For Manual Update:

- Make sure that you cut and paste the entire feature key text.
- The first line of the feature key must be “Serial Number: B0Exxxxxxxxxx”.
- The last line of the feature key is a long line of characters starting with “Signature: “.

For Automatic Update:

- Make sure you have a valid LiveSecurity account and you have registered your device serial number.
- You must have an Internet connection to retrieve your feature key.
- Make sure communications are not blocked by a network firewall.

Remove a Feature Key

You may need to remove a feature key after an XCS device evaluation or to troubleshoot license issues.

> ***Note*** *If you remove a feature key, you disable all security features and the system stops processing messages.*

To remove an existing feature key:

1. Select **Administration > System > Feature Key**.
   The Feature Key page appears.
2. Click **Remove**.
   A confirmation dialog box appears.
3. Click **OK** to confirm.

Feature Key Expiration

The WatchGuard XCS sends notifications to the administrator at 90, 60, 30, 7, 2, and 1 days before a feature key expires. To make sure your XCS operates with full functionality, update your feature key before the expiration date.

When a feature key expires on the WatchGuard XCS, the device continues to process and deliver mail, but expired features do not scan or perform actions on messages. Also, you will not receive software and Anti-Spam updates from Security Connection.

For example, if the Anti-Virus scanning feature key expires, the WatchGuard XCS continues to process mail, but the messages are not scanned for viruses.

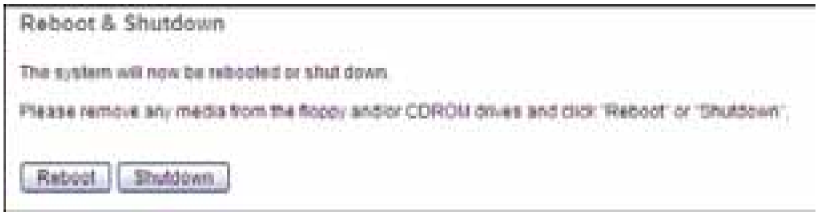
These features do not have associated expiration periods because they are required for normal system operations and management:

- Email
- Clustering
- Queue Replication
- Centralized Management

Reboot and Shutdown

To safely reboot or shut down the system:

1. Select **Administration > System > Reboot & Shutdown**.



Reboot & Shutdown

The system will now be rebooted or shut down

Please remove any media from the floppy and/or CDROM drives and click "Reboot" or "Shutdown"

2. To shut down the device and reboot, click **Reboot**.

   To shut down the device completely, click **Shutdown**.

> ***Note*** *Before you shut down the XCS device, remove any media from the CD-ROM drive.*

Security Connection

Security Connection is a service that polls WatchGuard's support servers for new updates, security alerts, and Anti-Spam database updates. The WatchGuard XCS sends a notification to the administrator when new information and updates are available.

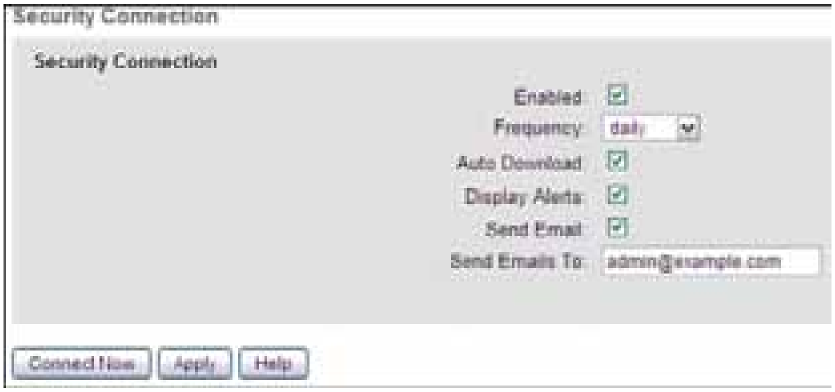
The Security Connection service is enabled by default after you install the WatchGuard XCS to make sure you automatically receive notifications for the latest software updates. After the initial installation, Security Connection immediately checks for new available updates. The Security Connection downloads any available updates for your system, but does not automatically install them.

To install software updates, from the Web UI, select **Administration > Software Updates > Updates**. See *Software Updates* for more detailed information on Software Updates.

> ***Note*** *For security purposes, all Security Connection files are encrypted and contain an MD5-based digital signature that is verified after the file is decrypted.*

To configure Security Connection:

1. Select **Administration > Software Updates > Security Connection**.



Security Connection

Security Connection

Enabled: ☑
Frequency: daily
Auto Download: ☑
Display Alerts: ☑
Send Email: ☑
Send Emails To: admin@example.com

2. Select the **Enabled** check box.
3. From the **Frequency** drop-down list, select how often to run the Security Connection service: **daily**, **weekly**, or **monthly**.

4. To enable software updates to be downloaded automatically, select the **Auto Download** check box.
   Updates are automatically downloaded, but not automatically installed. You must use Software Updates to manually install the updates.
5. To enable Security Connection alert messages to appear on the system console, select the **Display Alerts** check box.
6. To send an email to the address specified in the **Send Emails To** text box, select the **Send Email** check box.
7. In the **Send Emails To** text box, type the email address to receive notifications.
8. Click **Apply**.
9. Click **Connect Now** to run Security Connection and check for new software updates.

Software Updates

To make sure your device software is up to date with the latest patches and upgrades, you must install any updates released for your version of software.

After the installation of the WatchGuard XCS, Security Connection immediately checks for new software and automatically downloads any available updates. The Security Connection does not automatically install these updates. You must manually install them on the **Software Updates** page.

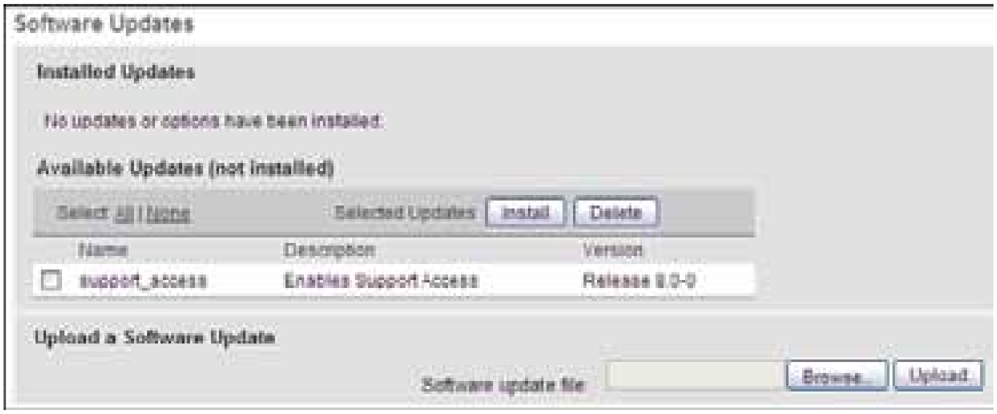
Updates appear in two sections: *Available Updates* (on the device, but not yet installed) and *Installed Updates* (installed and active). You can install an available update, or delete an installed update. Software updates downloaded from Security Connection appear in the *Available Updates* section.

> ***Note*** *We recommend that you back up the current system before you perform a software update. See Backup and Restore for detailed information on the backup and restore procedure.*

Install a Software Update

To install software updates:

1. Select **Administration > Software Updates > Updates**.
   The Software Updates page appears.



Software Updates

Installed Updates

No updates or options have been installed.

Available Updates (not installed)

Select: All | None   Selected Updates [Install] [Delete]

	Name	Description	Version
□	support_access	Enables Support Access	Release 9.0-0

Upload a Software Update

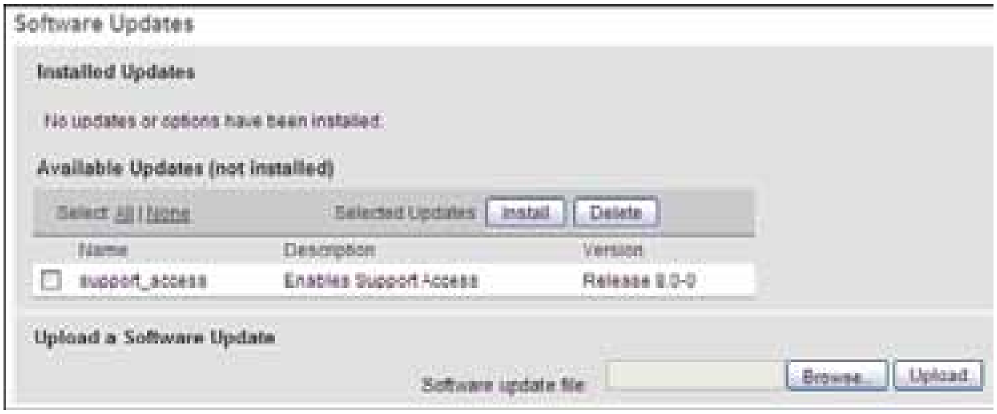
Software update file [ ] [Browse...] [Upload]

2. If you manually downloaded your software update:
   - Click **Browse** and select the software update.
   - Click **Upload**.
     The software update appears in the Available Updates section.
3. In the **Available Updates** section, select the software update.
4. Click **Install**.
   After you install updates, you must restart the device.

Delete a Software Update

To delete software updates:

1. Select **Administration > Software Updates > Updates**.
   The Software Updates page appears.



Software Updates

Installed Updates

No updates or options have been installed.

Available Updates (not installed)

	Name	Description	Version
□	support_access	Enables Support Access	Release 8.0-0

Upload a Software Update

Software update file

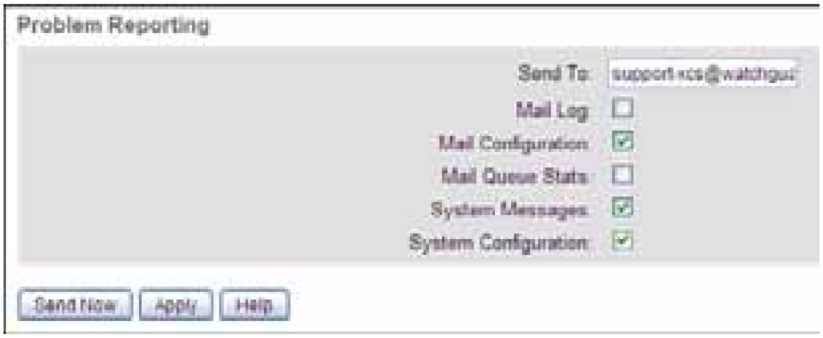
2. In the **Installed Updates** section, select the software update to delete.
3. Click **Delete**.
   After you delete the update, you must restart the device.

Problem Reporting

Problem reporting allows you to send important configuration and log information to WatchGuard Technical Support for help with troubleshooting device issues. This feature is intended for use in conjunction with an existing support request with technical support.

To configure Problem Reporting:

1. Select **Support > Problem Reporting**.
   The Problem Reporting page appears.



Problem Reporting

Send To: support-xcs@watchgua

Mail Log ☐

Mail Configuration ☑

Mail Queue Stats ☐

System Messages ☑

System Configuration ☑

2. In the **Send To** text box, type an email address to which to send the reports.
   The default address is WatchGuard Technical Support, but you can also enter your own email address so that you can view them before you send them to WatchGuard.
3. Select the **Mail Log** check box to send the latest hourly mail log.
4. Select the **Mail Configuration** check box to send your current mail configuration file.
5. Select the **Mail Queue Stats** check box to send a snapshot of the latest current mail queue statistics.
6. Select the **System Messages** check box to send the latest hourly system log.
7. Select the **System Configuration** check box to send a text version of the system configuration.
8. Click **Apply** to save the configuration.
9. Click **Send Now** to send the information to the configured email address.

Performance Tuning

There are several factors that can affect the performance of the WatchGuard XCS system:

- Network bandwidth
- Number of concurrent Mail and Web connections
- Number of background processes running, for example, Reporting and WebMail
- Internet unpredictability: Mail can often arrive in bursts of activity, with only a few messages arriving one minute, and several hundred the next. In the event of a network outage, for example, a failed router, the amount of queued mail that arrives after the router is back online can be very large
- Internet performance: Mail and Web clients can be very slow at connecting, and the connection may be disconnected before it is complete
- The time to process a message is also affected by the size of the email and its attachments
- Amount of system resources (Processing power, RAM, and disk space)

You must carefully consider these factors when you tune an XCS device for optimal performance. If your device is optimized for throughput to handle high mail loads, other aspects of the system may suffer from increased latency issues, for example, reporting, WebMail access, and the possibility of dropped connections by clients that cannot connect to a busy system. Similarly, allocating too many resources to resolve latency issues affects mail throughput performance.

> ***Warning*** *If you modify certain parameters, this can affect the performance of other aspects of the system, and we recommend that you only change these settings to resolve specific performance issues with guidance from WatchGuard Technical Support. Do not experiment with these settings.*

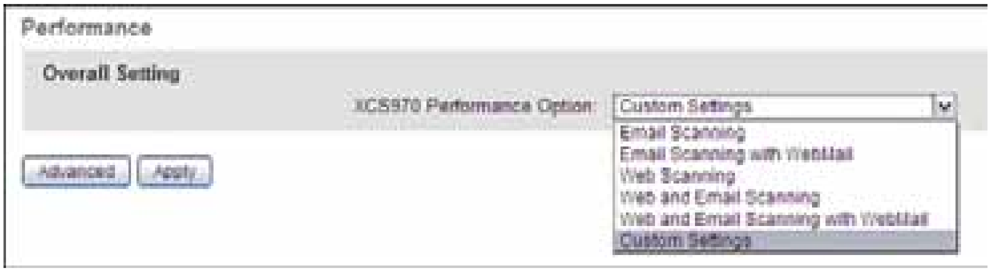
Select Performance settings

To configure performance settings:

1. Select **Configuration > Network > Performance**.
2. From the **Performance Option** drop-down list, select the type of performance profile to apply to the system:

   - Email Scanning
   - Email Scanning with WebMail
   - Web Scanning
   - Web and Email Scanning
   - Web and Email Scanning with WebMail
   - Custom

3. Click **Advanced** if you need to adjust any of the individual parameters to create a custom setting.



Performance

Overall Setting

XCS970 Performance Option: Custom Settings

Maximum Number of Processes

This parameter specifies the maximum number of concurrent processes that use mail services. This setting limits the number of connections accepted by smtpd, and the number of outgoing SMTP connections. If this number is set too large, you can run out of swap space.

Maximum Number of Parallel Deliveries

This parameter specifies the maximum number of outgoing SMTP connections to the same destination. This setting helps limit the number of outgoing connections. The value must be less than the maximum number of processes, or performance is degraded.

Maximum Number of Mail Scanners

This parameter specifies the maximum number of mail scanners that can run simultaneously. This setting limits the overall mail processing and memory footprint. Setting this value too high or too low may result in reduced performance. Valid settings are from 2 - 20.

Raise Priority of Heavy Weight Processes

Increasing the priority of heavyweight processes can increase performance and WebMail response times, but it can reduce the processing resources for other mail processes if it is set too high. Valid settings are from a default priority of 0 to a maximum priority of 20.

Number of Heavy Weight Processes

This parameter specifies the maximum number of heavy weight mail scanning processes that can be run simultaneously. Valid settings are: 1 (Default) to 6 (maximum processes). Setting a value greater than 2 does not improve performance, and we recommend you do not change this value from the default setting.

Number of DB Proxies

This parameter specifies the maximum number of database proxies that can be used by the mail scanning processes. This value is relative to the **Maximum Number of Processes** setting, and you must increase this value in conjunction with the number of maximum processes. Valid settings are from 2 (Default) to 12 (maximum processes), however, setting this value above 8 results in diminishing performance returns.

SMTP Connect Timeout

This SMTP parameter specifies the amount of time, in seconds, for an SMTP client to complete a TCP connection before the connection is dropped. This value defines how long the system waits for a response before timing out. The default is 0, but there is an overall system timeout of 5 minutes for SMTP connections. Increase this value to help with sites that have a slow Internet connection.

SMTP HELO Timeout

This SMTP parameter specifies the amount of time, in seconds, to receive the SMTP greeting banner before the XCS device drops the connection. The default is 300 seconds, which means that the system waits 5 minutes to receive the initial SMTP HELO message before it times out. Use a lower timeout value to increase performance by freeing up more connections. Increase this value to help with sites that have a slow Internet connection.

SMTPD Timeout

This SMTP parameter specifies the amount of time, in seconds, to send an SMTP server response and to receive an SMTP client request before the XCS device drops the connection. The default is 300 seconds. When the system connects to another mail server to deliver mail, it drops the connection if it takes more than 5 minutes to receive a response. A lower value can increase performance by freeing up connections. Increase this value to help with sites which have a slow Internet connection.

SMTPD Minimum Receive Rate

The minimum rate, in bytes per second, at which a client must send data. The limit is enforced after the SMTPD minimum receive rate interval has elapsed. Set this option to a higher value when excessively slow clients limit device resources. A value of 0 indicates no minimum rate. Default is 0.

SMTPD Receive Rate Interval

The time interval, in seconds, that must elapse before the SMTPD minimum receive rate restriction is enforced for a newly connected client. Set this to a higher value to provide clients more time to establish an acceptable data flow rate. A value of 0 means that the limit is enforced immediately. Default is 0.

Client connection count limit

The maximum number of simultaneous SMTP connections allowed from a single client IP address. Set to 0 for no limit. The default value is 50.

SMTP Tarpit Time

The amount of time, in seconds, to wait before replying to an SMTP client with a 4xx or 5xx error message (for example, the message content was rejected.) The default is 0 seconds. The tarpit time must be set to 0 for environments that reject a high number of SMTP connections. Low values can free up connections to improve performance. Higher values can deter senders from sending invalid content, for example, spam and viruses.

Service Throttle Time

The amount of time, in seconds, to wait before re-starting a messaging service that exits unexpectedly. The default is 60 seconds, and must be a minimum of 1 second.

Enable SMTP Connection Cache

Connection caching can improve delivery performance, primarily in deliveries to destinations with multiple mail servers where some of the servers are not responding. The system caches the responding servers and use those servers in the next delivery attempt. This option is disabled by default. If you enable this option, connection caching can introduce additional processing overhead and reduce performance in certain cases. Disable this option if performance issues occur.

Number of Concurrent Web Proxies

Increase the number of web proxy processes on the system to increase parallel processing of web requests and reduce client latency. Too many parallel requests can overload the scanning engine which results in various user requests blocking each other and contending for access. The preconfigured defaults are optimized based on the CPU and memory of the hardware platform. This value can be set from 1 to 32.

Number of Concurrent Web Scanners

Increase the number of concurrent web scanners on the system to increase parallel processing in the web scanning engine. Too many parallel scanners can overload the system and use too many resources. We recommend that this value match the **Number of Concurrent Web Proxies** setting. The preconfigured defaults are optimized based on the CPU and memory of the hardware platform. This value can be set from 1 to 32.

Maximum Number of Web Content Scanners

Sets the maximum number of web content scanners that can run simultaneously. This setting limits the overall proxy processing and memory footprint. This value can be set from 1 to 50.

Queue Threshold for Web Requests Per Proxy Instance

This setting limits the number of queued HTTP requests a single instance of the web proxy can have. In conjunction with the **Number of Concurrent Web Proxies** value, this setting determines the maximum number of concurrent web requests that can be handled by the system. Very high values for thresholds can adversely affect system resources, while low values may not be sufficient to handle the web traffic load for your environment. Error messages occur in the logs when a given proxy instance exceeds the configured limit. This value can be set from 1 to 20000. The default is 1000.

In-Memory Web Cache Size Mark

These are advanced settings for the web cache and they must be modified with caution.
The In-memory Web Cache sizes represent the thresholds used for cleaning up the memory cache. The low mark represents the memory level (in MB) after which the process starts cleaning up its entries. The critical mark represents the memory level (in MB) after which the process starts aggressively cleaning up its entries. The high mark represents the maximum memory (in MB) the in-memory web cache utilizes.

Mark	Default Recommended Value
Low	64 MB
Critical	128 MB
High	256 MB

Size of Temporary Files Filesystem

Specify the size of the /tmp file system at system startup. This setting affects the maximum size of attachments that are scanned, and must only be used if you are having problems with scanning large files. If you increase this setting beyond the amount of physical RAM, you can degrade device performance because of excessive swapping. You must monitor your system performance if you use this setting.

Size of Shared Memory block Allocated to Database

Specify the size of the shared memory block to make available to the database. Increase this value to increase the speed of database operations at the cost of having less memory available for other purposes. Increase this value if you are increasing the number of messages that are stored in the email database. If you change the size of the temp file system or shared memory block, you must restart the system before these settings take effect.

21 Monitoring

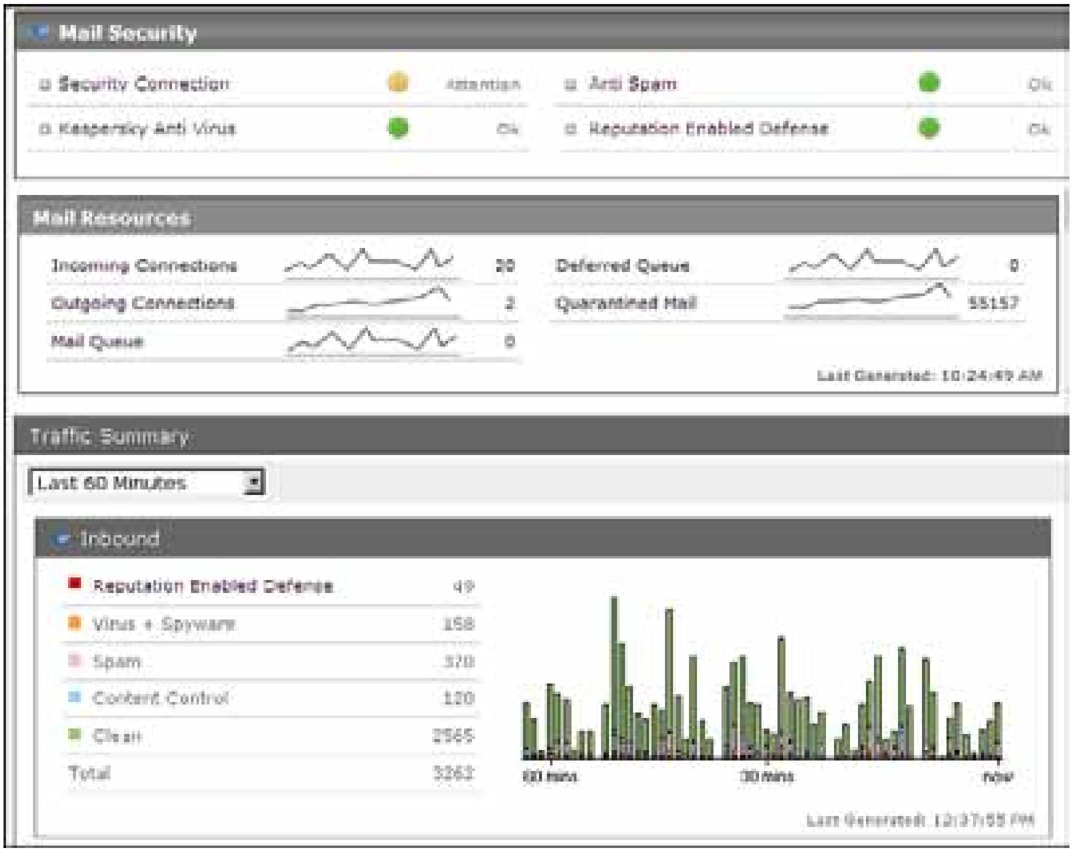
Dashboard

The WatchGuard XCS system *Dashboard* provides administrators with a brief statistical and graphical summary of current inbound and outbound email and web activity to enable rapid assessment of the current status of the WatchGuard XCS. The Dashboard contains links to these components:

- **Mail Summary** – Displays information on the status of your Mail Security features and your Mail Resources, for example, current incoming and outgoing connections, and the number of messages in the Mail, Deferred, and Quarantined queues. This page also provides a traffic summary of inbound and outbound mail traffic separated by category (for example, Virus, Spam, and Clean mail).
- **Web Summary** – Displays a web traffic summary separated by category (for example, URL Categorization and Spyware). The Web Summary page also provides information on the number of current active web connections, and the web cache efficiency. The Web Statistics page displays the top browsed categories, top five blocked web sites and users, and top five browsing users and browsed web sites. A Web User's page displays web statistics for individual users.
- **Recent Mail Activity** – Displays the most recent mail messages that have been processed by the system. This includes the Message ID, Sender and Recipient information, the message Status, and the final Action taken on the message.
- **Recent Web Activity** – Displays the most recent blocked web messages that have been processed by the system. This includes the Request ID, Request To and From information, the message Status, and the final Action taken on the request.
- **System Summary** – Displays the status of critical aspects of your WatchGuard XCS, for example, its software version and uptime, users logged in, disk/swap/CPU usage, RAID status, and server status.

> **Note** *In a cluster, the Dashboard only shows activity for the local system, and not for the entire cluster.*
> *For information and statistics for the entire cluster, see the Cluster Activity page.*

To see the Dashboard, go to **Activity > Status > Dashboard**.



Mail Security

Security Connection	●	Attention
Anti Spam	●	Ok
Kaspersky Anti Virus	●	Ok
Reputation Enabled Defense	●	Ok

Mail Resources

Incoming Connections	20
Outgoing Connections	2
Mail Queue	0
Deferred Queue	0
Quarantined Mail	55157

Last Generated: 10:24:49 AM

Traffic Summary

Last 60 Minutes

Inbound

🟥 Reputation Enabled Defense	49
🟧 Virus + Spyware	158
🟪 Spam	370
🟦 Content Control	120
🟩 Clean	2565
Total	3263

Last Generated: 12:37:55 PM

You can set the Dashboard to display its information based on a time period you select (**Last 60 Minutes**, **Last 24 Hours**, **Last 7 Days**, and **Last 31 Days**). Information on the Dashboard is updated every 60 seconds when the default, **Last 60 Minutes**, is selected. The page is updated hourly if set to **Last 24 Hours**, and updated every 24 hours if set to **Last 7 Days** and **Last 31 Days**.

> ***Note*** *Processed messages are not reflected in the statistics until the required time frame is summarized, for example, 60 seconds for "Last 60 Minutes", or one hour for "Last 24 Hours". The "Last Generated" time indicates when the statistics were last refreshed.*

Mail Security Status

The *Mail Security* section displays information on the status and licensing information for the WatchGuard XCS security features. You can expand each item to view the status details and the last connection time for each service.

> ***Note*** *The Mail Security status does not appear on a cluster client device. In addition, Reputation Enabled Defense status is only available on the Primary cluster device.*

- **Security Connection** – Indicates the status of communications with the Security Connection service:
  - **Green**: (OK status). Indicates that a successful connection has been made to Security Connection since the previous connection.

    - **Yellow**: (Attention status)
        - The system has not made a successful connection to Security Connection since the last scheduled attempt.
    - **Red**: (Urgent status)
        - The system has not made a successful connection to Security Connection in the last three scheduled attempts.
    - **Grey**: (Disabled). The Security Connection feature is disabled.
- **Kaspersky Anti-Virus** – Indicates the status of the Anti-Virus scanning feature:
    - **Green**: (OK status). The most recent Anti-Virus pattern update is between 0 and 26 hours old.
    - **Yellow**: (Attention status)
        - The most recent Anti-Virus pattern update is between 26 and 50 hours old.
    - **Red**: (Urgent status)
        - The most recent Anti-Virus pattern update is more than 50 hours old.
        - The Anti-Virus feature license is expired.
    - **Grey**: (Disabled or not licensed). Indicates that the Anti-Virus feature is disabled or is not licensed.
- **Anti-Spam** – Indicates the status of the Intercept Anti-Spam feature:
    - **Green**: (OK status). The most recent Anti-Spam database update is less than a month old.
        - DNS and URL Block List lookup status is OK.
    - **Yellow**: (Attention status)
        - The most recent Anti-Spam pattern update is 31 to 62 days old.
        - There is an issue with DNS and/or URL Block List primary or alternate server lookups.
    - **Red**: (Urgent status)
        - The most recent Anti-Spam pattern update is more than 62 days old.
        - There is an issue with DNS and/or URL Block List primary and alternate server lookups.
- **Reputation Enabled Defense** – Indicates the status of the RED feature:
    - **Green**: (OK status). Indicates the RED server status is OK.
    - **Yellow**: (Attention status). Indicates there is an issue connecting to a specific RED server.
    - **Red**: (Urgent status)
        - Indicates there is an issue connecting to the RED service.
        - The RED license has expired.
    - **Grey**: (Not licensed or disabled).
        - The RED feature is not licensed.
        - The RED feature is disabled.
- **McAfee Anti-Virus (If licensed)** – Indicates the status of the McAfee Anti-Virus feature:
    - **Green**: (OK status). The most recent McAfee Anti-Virus pattern update is between 0 and 26 hours old.
    - **Yellow**: (Attention status). The most recent McAfee Anti-Virus pattern update is between 26 and 50 hours old.
    - **Red**: (Urgent status)
        - The most recent McAfee Anti-Virus pattern update is more than 50 hours old.
        - The Anti-Virus feature license is expired.
    - **Grey**: (Disabled). Indicates that the McAfee Anti-Virus feature is disabled.
- **Brightmail Anti-Spam (if licensed)** – Indicates the status of the Brightmail Anti-Spam feature:
    - **Green**: (OK status). The most recent Brightmail Anti-Spam pattern update is between 0 and 26 hours old.
    - **Yellow**: (Attention status). The most recent Brightmail pattern update is between 26 and 50 hours old.
    - **Red**: (Urgent status)

        - The most recent Brightmail Anti-Spam pattern update is greater than 50 hours old.
        - The Brightmail Anti-Spam feature license is expired.
    - **Grey**: (Disabled). Indicates that the Brightmail Anti-Spam feature is disabled.

- **SecureMail Encryption (if licensed)** – Indicates the status of the SecureMail email encryption feature:
    - **Green**: (OK status). The SecureMail service is enabled and can connect to SecureMail servers.
    - **Red**: (Urgent status)
        - The SecureMail service is enabled, but cannot connect to SecureMail servers.
        - The SecureMail feature license is expired.
    - **Grey**: (Not licensed or disabled).
        - The SecureMail feature is disabled
        - The SecureMail feature is not licensed.

Mail Summary

The *Mail Summary* statistics page displays information on mail traffic that passes through the system and contains statistics on Mail Resources and a Mail Traffic Summary.

Mail Resources

The *Mail Resource* statistics are updated every 60 seconds. The corresponding activity graphs are updated every hour.

- **Incoming Connections** – Displays the current amount of incoming mail connections to this system.
- **Outgoing Connections** – Displays the current amount of outgoing mail connections from this system.
- **Mail Queue** – Indicates how many messages are currently in the Mail Queue waiting to be delivered. View and manage these messages in **Activity > Queue/Quarantine > Mail Queue**.
- **Deferred Queue** – Indicates the number of messages that have had their delivery deferred because of unavailability of the destination mail server. The system tries to deliver these messages at a later time. You can configure this option in **Configuration > Mail > Delivery**.
- **Quarantined Mail** – Indicates the number of messages that have been sent to the administrative quarantine area. View and manage messages in **Activity > Queue/Quarantine > Message Quarantine**.

Mail Traffic Summary

The *Traffic Summary* section displays a graph that shows how many inbound and outbound email messages have been processed by the system.

You can customize the Traffic Summary display to show statistics for the last 60 minutes, 24 hours, 7 days, or 31 days with the drop-down list. Information on the Dashboard is updated every 60 seconds when the default, **Last 60 Minutes**, is selected. The page is updated hourly if set to **Last 24 Hours**, and updated every 24 hours if set to **Last 7 Days** and **Last 31 Days**.

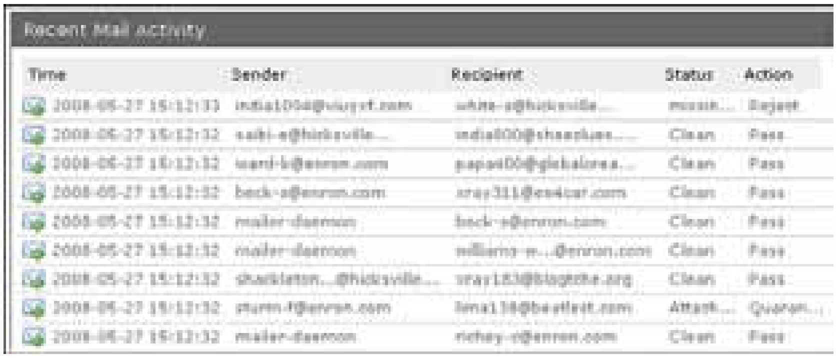
These statistics are displayed:

- **Reputation Enabled Defense** – Indicates the number of messages that were rejected by Reputation Enabled Defense and other features that reject a message before the SMTP connection is complete. This category is displayed for inbound mail only. This statistic includes these connection rejects:
    - Reputation Enabled Defense Connection Reject (Reputation, Infection, and Dial-up)

  - DNS Block List Reject
  - Threat Prevention Reject
  - Specific Access Pattern Reject
  - Pattern Filter reject
  - Connection Rule reject
  - Reject on unauthorized SMTP pipelining
  - Reject on unknown sender domain
  - Reject on missing reverse DNS
  - Reject on missing sender MX
  - Reject on non FQDN sender
  - Reject on Unknown Recipient
  - Reject on missing addresses
  - Reject if number of recipients exceeds maximum
  - Reject if message size exceeds maximum
- **Virus + Spyware** – Indicates the amount of messages that contained viruses, spyware, or were malformed.
- **Spam** – Indicates the number of messages that have been classified as spam. This includes Certainly Spam, Probably Spam, Maybe Spam, Brightmail spam, Reputation Enabled Defense spam, and DNS Block List Spam. This category is displayed for inbound mail only. This category also depends on the spam logging configuration in **Configuration > Miscellaneous > Reports**. The spam action of **Just Log** is counted in the total if it is enabled in the spam logging configuration.
- **Content Control** – Indicates the number of messages that have had their content classified by the Content Control features, for example, Attachment Control, Content Scanning, Pattern Filters, Content Rules, Document Fingerprinting, and Objectionable Content Filtering.
- **Clean** – Indicates the number of messages processed by the system that have passed all security, spam, and content checks. This includes messages that have been detected by these features but have an action of **Just Log**.

Recent Mail Activity

The *Recent Mail Activity* page displays information on the most recent mail messages that have passed through the system. The data updates every 60 seconds and also updates when you refresh the page.



Recent Mail Activity

Time	Sender	Recipient	Status	Action
2008-05-27 15:12:33	india1004@viuyrf.com	white-a@hicksville...	missin...	Reject
2008-05-27 15:12:32	saibi-e@hicksville...	india800@shaarbues...	Clean	Pass
2008-05-27 15:12:32	ward-k@enron.com	papad00@globalarea...	Clean	Pass
2008-05-27 15:12:32	beck-s@enron.com	xray311@ex4car.com	Clean	Pass
2008-05-27 15:12:32	mailer-daemon	beck-s@enron.com	Clean	Pass
2008-05-27 15:12:32	mailer-daemon	williams-w...@enron.com	Clean	Pass
2008-05-27 15:12:32	shackleton...@hicksville...	xray183@blogethe.org	Clean	Pass
2008-05-27 15:12:32	sturm-f@enron.com	lima138@beatlest.com	Attach...	Quaran...
2008-05-27 15:12:32	mailer-daemon	richey-c@enron.com	Clean	Pass

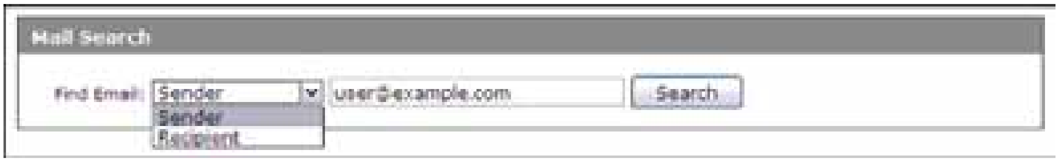
- **Time** – Indicates when the message was processed by the system.
- **Sender** – Indicates the email address of the sender of the mail message.
- **Recipient** – Indicates the email address of the recipient of the mail message.

- **Status** – Indicates which feature acted upon the message if a security or content check was triggered. For example, *OCF* indicates that the message was acted on by the Objectionable Content Filter.
- **Action** – The final action that was taken on the message after it was processed, for example, *Reject*.

Each message that passes through the XCS device has a unique message identification number. Hover over the icon to the left of the message to see the Queue ID for the message. Click the icon to see the processing details for the message.

To search the recent mail activity:

1. From the **Find Email** drop-down list, select **Sender** or **Recipient**.



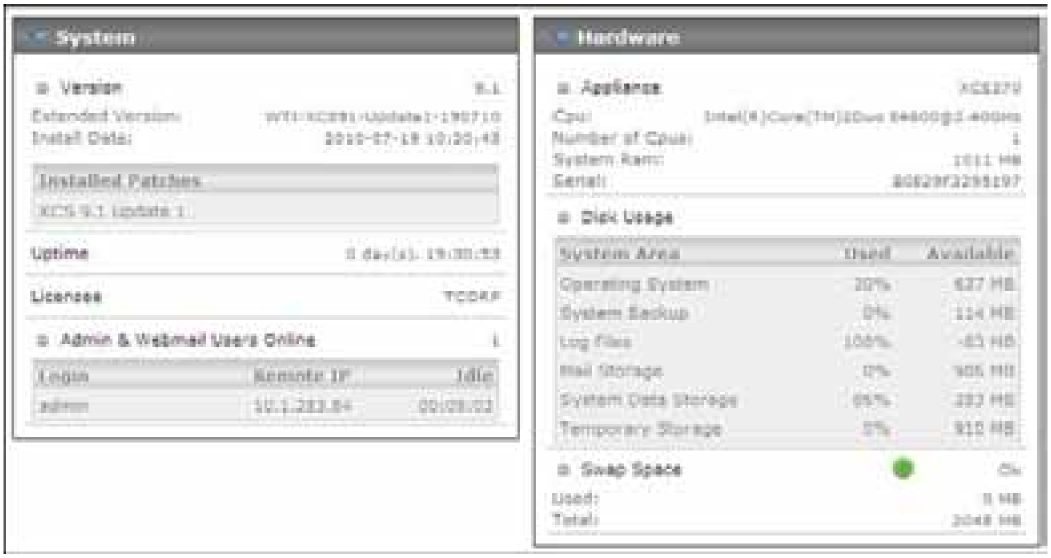
2. In the **Find Email** text box, type a search term that exactly matches the sender or recipient email address.

   For example, `user@example.com`.

3. Click **Search**.
   The Message History page appears with the search results.

System Summary

The *System Summary* page displays the status of critical aspects of your WatchGuard XCS, for example, its software version and uptime, users logged in, disk/swap/CPU usage, RAID status, and server status.



System

Version 9.1
Extended Version: WTI-XCS91-Update1-190710
Install Date: 2010-07-19 10:20:43

Installed Patches
XCS 9.1 Update 1

Uptime 0 day(s), 19:30:53

Licenses TCOKF

Admin & Webmail Users Online 1

Login	Remote IP	Idle
admin	10.1.203.64	00:09:03

Hardware

Appliance XCS270
Cpu: Intel(R)Core(TM)2Duo E4600@2.40GHz
Number of Cpus: 1
System Ram: 1011 MB
Serial: 80829F3295197

Disk Usage

System Area	Used	Available
Operating System	20%	627 MB
System Backup	0%	114 MB
Log Files	100%	-83 MB
Mail Storage	0%	905 MB
System Data Storage	05%	233 MB
Temporary Storage	0%	910 MB

Swap Space ● Ok
Used: 0 MB
Total: 2048 MB

System

- **Version** – Displays the current software version of the WatchGuard XCS. This includes the time of installation and any installed software patches.
- **Uptime** – Displays the amount of time since the last restart of the WatchGuard XCS.
- **Licensee** – Displays the licensed user of the WatchGuard XCS. This is the text entered as the *Organization Name* during the device installation.
- **Admin & WebMail Users Online** – Displays the number of users who are logged in through the web admin interface or through a WebMail session. Expand the status to view the login name, IP address, and idle time.

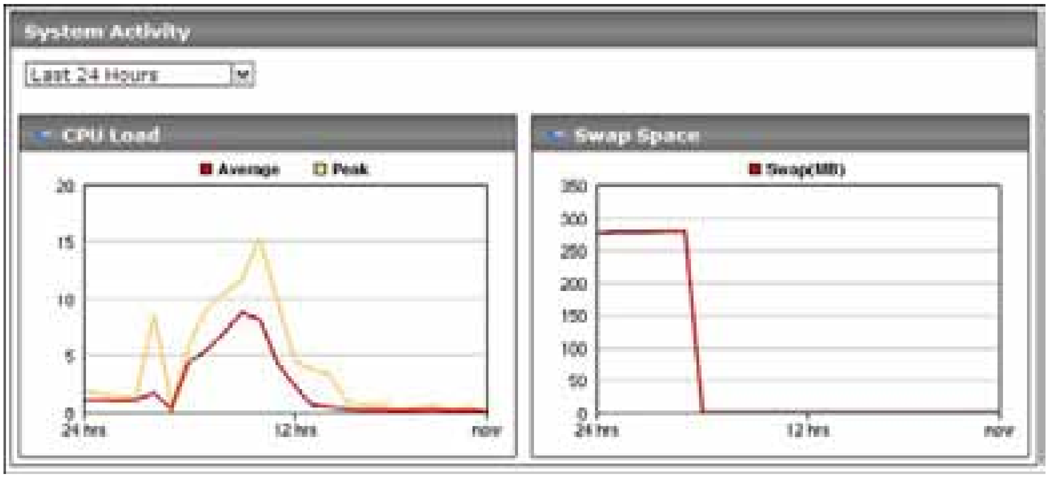
Hardware

- **Appliance** – Displays information on your hardware device model. Expand the status to view CPU information, the total amount of RAM memory, and the device serial number.
- **Disk Usage** – Expand the status to view the used and available space for each disk partition.
- **Swap Space** – Displays the current status for the amount of swap space on the system. Expand the status to view the total swap space and amount of swap space in use.
  - **Green**: (OK status). Indicates that the swap space being used is not greater than half of the available memory.
  - **Red**: (Urgent status). Indicates that the swap space being used is greater than half of the available memory.
- **RAID Status** – This displays the RAID status for hardware device models with a RAID disk system. Expand the status to view the controller, RAID Type, and RAID Size.
  - **Green**: (OK status)
  - **Yellow**: (Attention status). The RAID system is rebuilding.
  - **Red**: (Urgent status). The RAID system is degraded. This indicates a failed disk.

System Activity

You can display the CPU load and swap space statistics for these time periods: **Last 24 Hours**, **Last 7 Days**, and **Last 31 Days**.

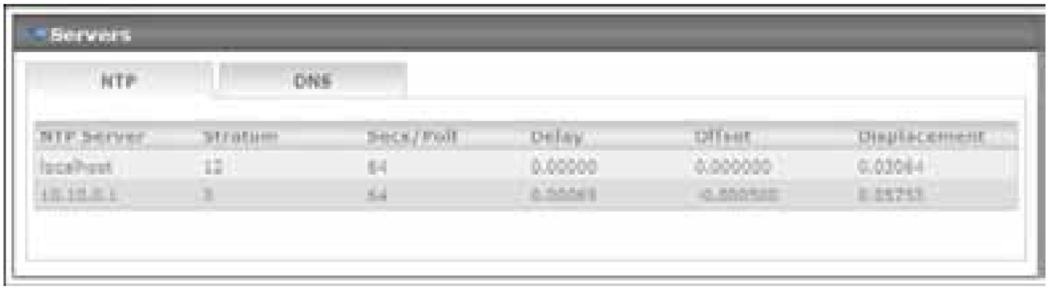
> ***Note*** *To display the last 31 days, the* ***Message History Days*** *option must be set to 31 in* ***Configuration > Miscellaneous > Reports****.*



- **CPU Load** – Displays the average and peak CPU load for the specified time period.
- **Swap Space** – Displays the amount of swap space usage (in MB) for the specified time period.

Servers

The *Servers* section displays the status of your configured NTP and DNS servers.



NTP Server	Stratum	Secs/Poll	Delay	Offset	Displacement
localhost	12	64	0.00000	0.000000	0.03064
10.10.0.1	3	64	0.00069	-0.000500	0.18755

- **NTP** – Displays the status of your configured NTP (Network Time Protocol) servers. This includes these statistics:
  - **NTP Server**: Displays the IP address of the NTP server. The local NTP server appears as “localhost”.
  - **Stratum**: Indicates the number of steps from a primary time source.
  - **Secs/Poll**: Indicates how many seconds between attempts to query the time server.
  - **Delay**: Indicates the round trip time of the time server query.
  - **Offset**: Indicates the difference between the reference time and the system clock.
  - **Displacement**: Indicates the amount of time difference between time server queries.
- **DNS** – Displays the status of your configured DNS (Domain Name Service) servers.
  - **Name Server**: Displays the IP address of the name server.
  - **Status**: Displays the current connection status to the name server:
    - **OK**: The DNS server is resolving domain names.
    - **Not OK**: The DNS server is not resolving domain names.

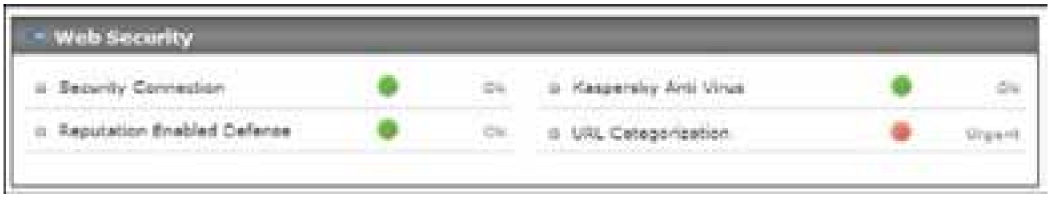
Web Summary

The *Web Summary* page includes the status of your web security features and displays statistics on web traffic that passes through the system. This page contains statistics on the types of Blocked Content, Connections, Web Cache Efficiency, Top 5 Blocked Web Sites and IP Addresses/Users, and Top 5 Browsed Web Sites and Browsing Users.

Web Security Status

The *Web Security* section displays information on the status and licensing information for the WatchGuard XCS web security features. You can expand each item to view the status details and the last connection time for each service.

> ***Note*** *The Web Security status does not appear on a cluster client device. In addition, Reputation Enabled Defense status is only available on the Primary cluster device.*



Web Security

Security Connection	🟢	Ok	Kaspersky Anti Virus	🟢	Ok
Reputation Enabled Defense	🟢	Ok	URL Categorization	🔴	Urgent

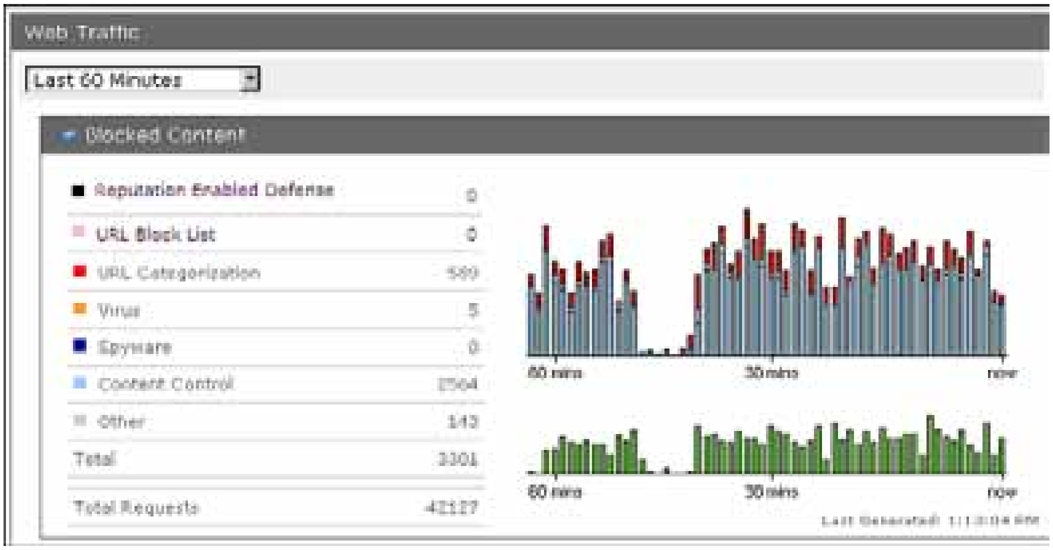
- **Security Connection** – Indicates the status of communications with the Security Connection service:
  - **Green**: (OK status). Indicates that a successful connection has been made to Security Connection since the previous connection.
  - **Yellow**: (Attention status)
    - The system has not made a successful connection to Security Connection since the last scheduled attempt.
  - **Red**: (Urgent status)
    - The system has not made a successful connection to Security Connection in the last three scheduled attempts.
  - **Grey**: (Disabled). The Security Connection feature is disabled.
- **Kaspersky Anti-Virus** – Indicates the status of the Intercept Anti-Virus feature:
  - **Green**: (OK status). The most recent Anti-Virus pattern update is between 0 and 26 hours old.
  - **Yellow**: (Attention status). The most recent Anti-Virus pattern update is between 26 and 50 hours old.
  - **Red**: (Urgent status)
    - The most recent Anti-Virus pattern update is more than 50 hours old.
    - The Anti-Virus feature license is expired.
  - **Grey**: (Disabled or not licensed). Indicates that the Anti-Virus feature is disabled or is not licensed.
- **Reputation Enabled Defense** – Indicates the status of the RED feature:
  - **Green**: (OK status). Indicates the RED server status is OK.
  - **Red**: (Urgent status)
    - Indicates there is an issue connecting to the RED service.
    - The RED/URL Categorization license has expired.
  - **Grey**: (Not licensed). The RED/URL Categorization feature is not licensed.

- **URL Categorization** – Indicates the status of the URL Categorization feature:
  - **Green**: (OK status). The most recent control list update was successful and is less than 1 week old.
  - **Yellow**: (Attention status).
    - The most recent control list update was successful and is between 1 and 2 weeks old.
    - Also indicates a control list download is in progress.
  - **Red**: (Urgent status)
    - URL Categorization is waiting for the initial Control List Update.
    - The most recent control list update was successful and is greater than 2 weeks old.
    - The control list update was not successful and failed to update.
    - The URL Categorization license is expired.
  - **Grey**: (Not licensed or disabled).
    - Indicates that the URL Categorization feature is not licensed.
    - Indicates the URL Categorization feature is disabled.

Web Traffic

The *Web Traffic* section contains information on the number of web requests and downloaded files that were blocked because of URL and content issues. This includes the current number of active connections that use the Web Proxy.

You can customize the Web Traffic display to show statistics for the last 60 minutes, 24 hours, 7 days, or 31 days from the drop-down list. Information on the Dashboard is updated every 60 seconds when the default, **Last 60 Minutes**, is selected. The page is updated hourly if set to **Last 24 Hours**, and updated every 24 hours if set to **Last 7 Days** and **Last 31 Days**.



■ Reputation Enabled Defense	0
■ URL Block List	0
■ URL Categorization	589
■ Virus	5
■ Spyware	0
■ Content Control	2564
■ Other	143
Total	3301
Total Requests	42127

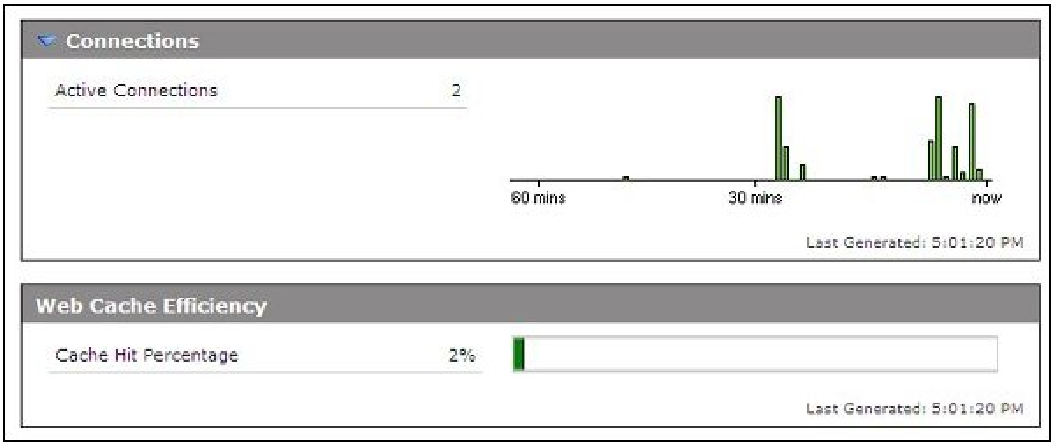
Blocked Content

- **Reputation Enabled Defense** – Indicates the number of web connections blocked because the web site URL received a poor reputation score from the Reputation Enabled Defense service.
- **URL Block List**– Indicates the number of web connections blocked because the web site URL appeared on a URL Block List.

- **URL Categorization** – Indicates the number of web connections that were blocked because the URL was in a URL Categorization list of blocked web sites.
- **Virus** – Indicates the number of web downloads and uploads that contained a virus.
- **Spyware** – Indicates the number of web downloads and uploads that contained spyware.
- **Content Control** – Indicates the number of web request uploads and downloads that were blocked because of content control issues detected by Attachment Control, Content Scanning, and Objectionable Content Filtering.
- **Other** – Indicates the number of web messages that were blocked because of other reasons that are not covered in the categories in this list. This includes the HTTP Blocked Sites List.

Connections

Indicates the number of active connections between the Web Proxy and external web servers. This includes a graph of the number of connections over the selected time period. This statistic is the average number of connections in the selected report period. For example, when **Last 60 Minutes** is selected, this indicates the average number of active connections every minute. If **Last 24 Hours** is selected, this indicates the average number of active connections per hour. If **Last 7 Days** or **Last 31 Days** is selected, this indicates the average number of active connections per day.



Connections

Active Connections 2

Last Generated: 5:01:20 PM

Web Cache Efficiency

Cache Hit Percentage 2%

Last Generated: 5:01:20 PM

Web Cache Efficiency

The XCS system contains a web cache that caches data and images from web sites visited by users of the Web Proxy. This improves performance and reduces bandwidth for subsequent visits to these web sites, as the data and images are read from the disk cache instead of retrieving data over the Internet. When a request is received, the system compares its cached data with the requested web site to make sure it has the latest data, and new web site updates are reflected in the disk cache.

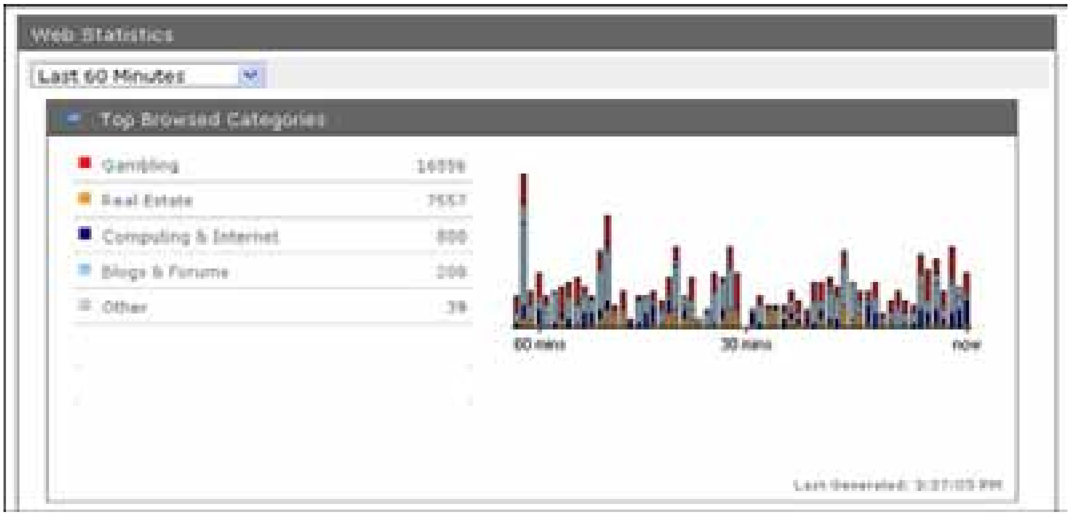
The *Web Cache Efficiency* counter indicates the percentage success (from 1 to 100) of data retrieval from the cache (a cache "hit"). Any requests that did not find the object in the web cache are sent out to the Internet to retrieve the content. The value increases after your system processes requests for at least 24-48 hours.

When it reaches a baseline level (typically between 15 to 20%), you can recognize changes in efficiency. If your efficiency gradually decreases, it can indicate your cache is corrupted and must be flushed (**Activity > Status > Utilities**). The Web Cache Efficiency percentage reflects information collected from the previous two weeks.

Web Statistics

The *Web Statistics* section contains information on the Top Browsed Categories, Top 5 Blocked Web Sites, Top 5 Blocked IP/Users, Top 5 Browsed web sites, and Top 5 Browsing Users.

You can customize the Web Statistics display to show statistics for the last 60 minutes, 24 hours, 7 days, or 31 days from the drop-down list. Information on the Dashboard is updated every 60 seconds when the default, **Last 60 Minutes**, is selected. The page is updated hourly if set to **Last 24 Hours**, and updated every 24 hours if set to **Last 7 Days** and **Last 31 Days**.



Web Statistics

Last 60 Minutes

Top Browsed Categories

🟥 Gambling	14559
🟧 Real Estate	7557
🟦 Computing & Internet	800
🟦 Blogs & Forums	208
▨ Other	39

Last Generated: 3:27:03 PM

Top Browsed Categories

This list indicates the top five web site categories that have had been blocked by URL Categorization. These statistics are only displayed if URL Categorization is enabled. The **Other** category indicates the total of all other categories.

Top 5 Blocked Users

This list indicates the top five IP addresses or users (if authentication is enabled) that have been blocked because of security and content issues, for example, viruses, spyware, content controls, URL Block Lists, HTTP Blocked Sites, and URL Categorization.

Top 5 Blocked Websites

This list indicates the top five web sites that have had been blocked because of security and content issues, for example, viruses, spyware, content controls, URL block lists, HTTP blocked sites, and URL Categorization.

Top 5 Browsing Users

Indicates the top five users with the most browse time. This value represents the total amount of browse time for the specific user from all of their browse time sessions. If authentication is enabled, the email address of the user is displayed. If authentication is disabled, the IP address of the user is displayed.

Top 5 Browsed Websites

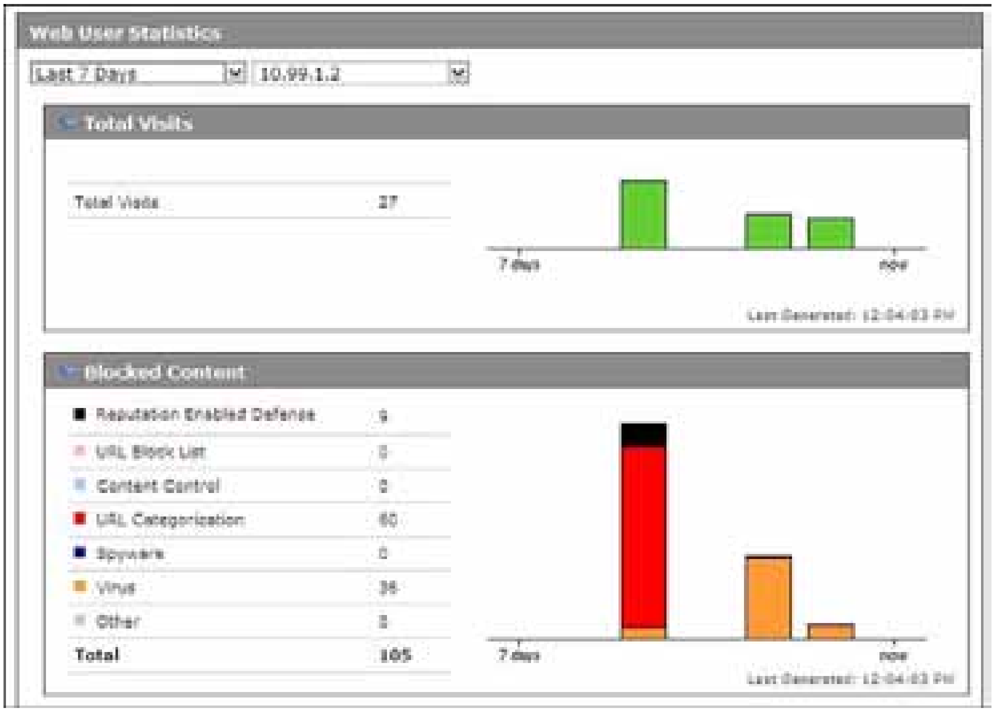
Indicates the top five most browsed web sites. The Browsed Websites value indicates specific web site *visits*. This statistic does not count each individual web site *hit* that results in hit counts for each retrieved image, and additional files from the same domain or an external domain. A single web site visit can include several *hits* to the same domain or external web site domain in a specific period of time.

Web Users

The *Web Users* section contains information on web browsing statistics for individual users. You can view Web User statistics for the last 24 hours, or for the last 7 days. The Web User statistics are updated every hour and reflect information collected up to the previous hour.

From the drop-down list, select an existing user to see their web statistics.

- Select a user name if authentication is enabled.
- Select an IP address if authentication is disabled.



Web User Statistics

Last 7 Days | 10.99.1.2

Total Visits

Total Visits	27

Last Generated: 12:04:03 PM

Blocked Content

■ Reputation Enabled Defense	9
■ URL Block List	0
■ Content Control	0
🟥 URL Categorization	60
■ Spyware	0
🟧 Virus	36
■ Other	0
Total	**105**

Last Generated: 12:04:03 PM

Total Visits

Indicates the total number of web site visits for the user. A *visit* is the domain to which the client sends a request. This statistic does not count each individual web site *hit* that results in hit counts for each retrieved image and other files from the same domain or to external domains. A single web site visit can include several *hits* to the same web site domain or other domains in a specific period of time.

Blocked Content

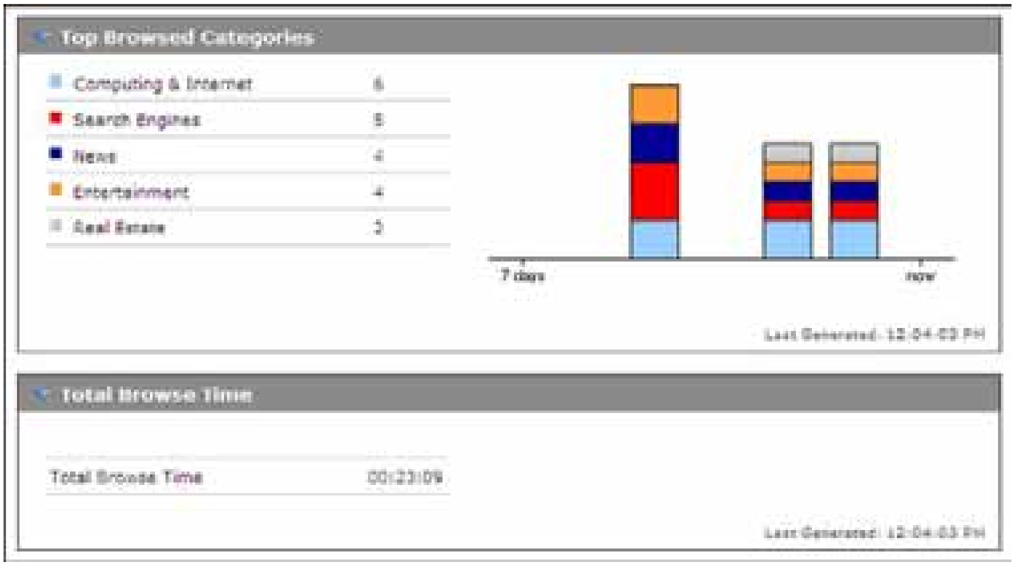
- **Reputation Enabled Defense**– Indicates the number of web connections blocked because the web site URL received a poor reputation score from the Reputation Enabled Defense service.
- **URL Block List**– Indicates the number of web connections blocked because the web site URL appeared on a URL Block List.
- **URL Categorization** – Indicates the number of web connections that were blocked because the URL visited was listed in a URL Categorization list of blocked web sites.
- **Virus** – Indicates the number of web downloads and uploads that contained a virus.
- **Spyware** – Indicates the number of web downloads and uploads that contained spyware.
- **Content Control** – Indicates the number of web request uploads and downloads that were blocked because of content control issues detected by Attachment Control, Content Scanning, and OCF.
- **Other** – Indicates the number of web messages that were blocked because of other reasons that are not covered in the categories in this list. This includes the HTTP Blocked Sites List.

Top Browsed Categories

This list indicates the top five web site categories that have had been blocked by URL Categorization. The **Other** category indicates the total of all other categories. These statistics are only displayed if URL Categorization is enabled.

Total Browse Time

Indicates the total amount of browse time for the specific user from all of their browse time sessions. The Total Browse Time is updated every hour and reflects information collected up to the previous hour.



Top Browsed Categories

Computing & Internet	6
Search Engines	5
News	4
Entertainment	4
Real Estate	3

Last Generated: 12:04:03 PM

Total Browse Time

Total Browse Time	00:23:09

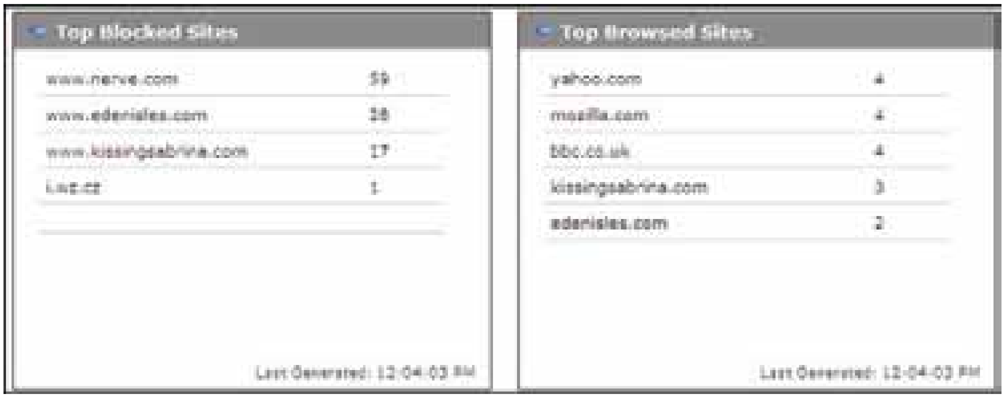
Last Generated: 12:04:03 PM

Top Blocked Sites

This list indicates the top five web sites that have had been blocked because of security and content issues, for example, viruses, spyware, content controls, URL block lists, HTTP blocked sites, and URL Categorization. The Top Blocked Sites are updated every 60 seconds, and reflect information collected from the last 7 days.

Top Browsed Sites

Indicates the top five most browsed web sites. The Browsed Websites value indicates specific web site *visits*. This statistic does not count each individual web site *hit* that results in hit counts for each retrieved image, subdomain files, and so on. A single web site visit may include several *hits* to the same web site domain in a specific period of time. The Top Browsed Sites are updated every hour and reflect information collected from the last seven days.



Top Blocked Sites

www.nerve.com	59
www.edenisles.com	28
www.kissingsabrina.com	17
live.cz	1

Last Generated: 12:04:03 PM

Top Browsed Sites

yahoo.com	4
mozilla.com	4
bbc.co.uk	4
kissingsabrina.com	3
edenisles.com	2

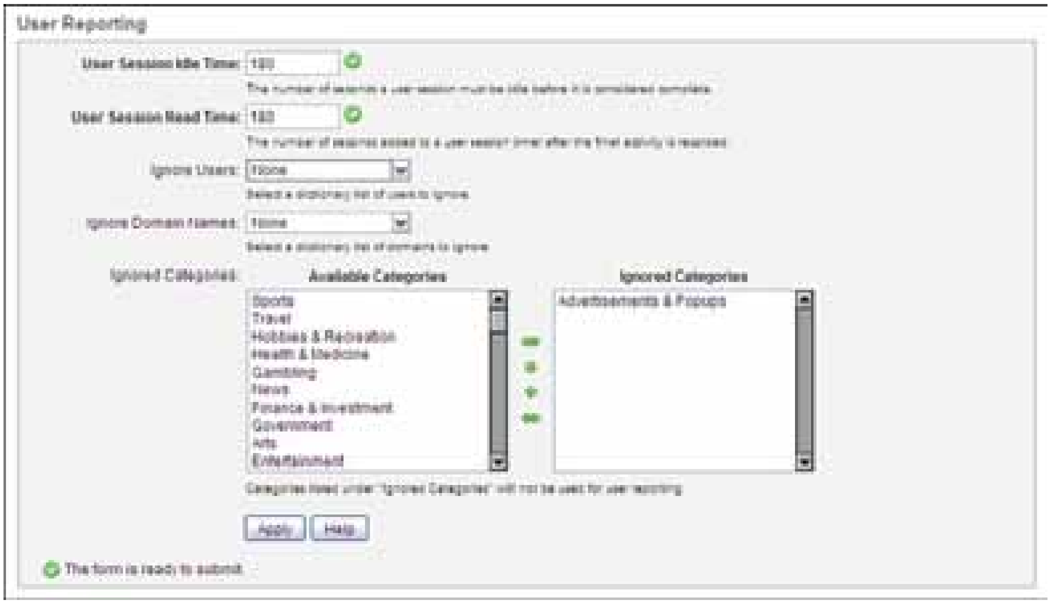
Last Generated: 12:04:03 PM

Web User Reporting Configuration

You can modify how the WatchGuard XCS calculates the browse time for a user, and define users, domains, and categories that are not reported on by the User Reporting feature.

To configure User Reporting:

1. Select **Configuration > Web > User Reporting**.



User Reporting

User Session Idle Time: 180

The number of seconds a user session must be idle before it is considered complete.

User Session Read Time: 180

The number of seconds added to a user session timer after the final activity is recorded.

Ignore Users: None

Select a dictionary list of users to ignore.

Ignore Domain Names: None

Select a dictionary list of domains to ignore.

Ignored Categories:

Available Categories	Ignored Categories
Sports Travel Hobbies & Recreation Health & Medicine Gambling News Finance & Investment Government Arts Entertainment	Advertisements & Popups

Categories listed under "Ignored Categories" will not be used for user reporting.

The form is ready to submit.

2. In the **User Session Idle Time** text box, type the number of seconds a user session must be idle before it is considered complete.

   When this time has passed, the user's session is written to the log files and considered a unique browse session. You can set a value from 10 to 3600 seconds. The default value is 180 seconds.

3. In the **User Session Read Time** text box, type the number of seconds added to a user session timer after the final activity is recorded.

   The read time is added to the user's browse-time to make sure time is allocated for viewing a web page after the last web page access. The **User Session Read Time** must be equal to or less than the **User Session Idle Time**. The default value is 180 seconds.

4. From the **Ignore Users** drop-down list, select a dictionary list of users that are not tracked by the User Reporting feature.

   The dictionary can contain a list of user names and IP addresses with one entry per line.

   For example,

   ```
   user@example.comuser2@example.com192.168.1.100
   ```

5. From the **Ignore Domain Names** drop-down list, select a dictionary list of domains that are not tracked by the User Reporting feature.

   The dictionary must contain a list of domains with one entry per line. Use a wildcard character “*” to include subdomains.

   For example,

   ```
   *.example.comexample2.comexample3.com
   ```

6. In the **Ignored Categories** section, select the URL Categorization web site categories that are not tracked by the User Reporting feature.

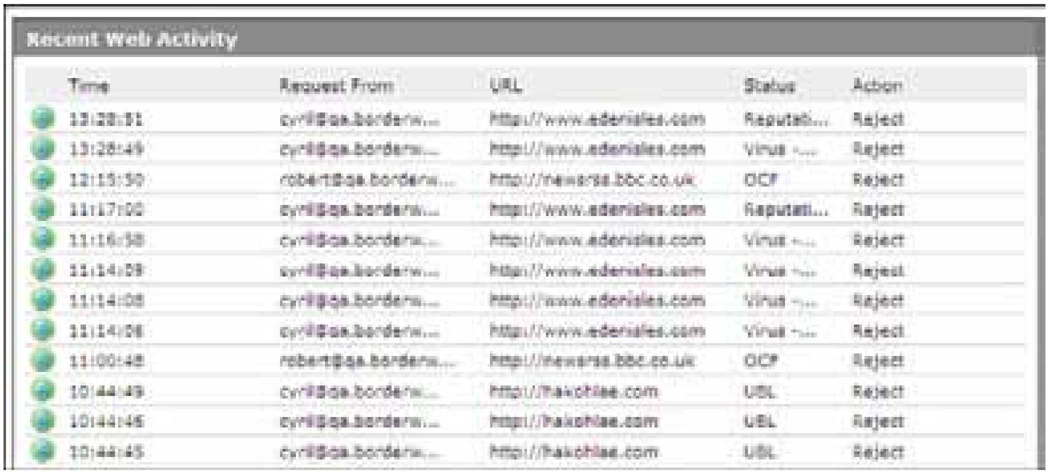
   This option requires that the URL Categorization feature be enabled.

   Use the arrow buttons to move categories from the *Available Categories* list to the *Ignored Categories* list.
7. Click **Apply**.

Recent Web Activity

The *Recent Web Activity* page displays information on the most recent blocked web requests that have passed through the system. The data updates every 60 seconds and also updates when the page is refreshed.

- **Time** – Indicates when the request was processed by the system.
- **Request From** – The source of the web request displayed as the user name and the IP address of the client. If authentication is not enabled, the user name displays *unknown user*.
- **Request To** – Indicates the destination URL of the web request.
  For example: http://www.example.com.
- **Status** – Indicates which feature acted upon the request if a security or content check was triggered. For example, a status of *OCF* indicates that the request was acted on by the Objectionable Content Filtering feature.
- **Action** – Indicates the final action that was taken on the request after it was processed, for example, *Reject*.



Recent Web Activity

Time	Request From	URL	Status	Action
13:28:51	cyril@qa.borderw...	http://www.edenisles.com	Reputati...	Reject
13:28:49	cyril@qa.borderw...	http://www.edenisles.com	Virus -...	Reject
12:15:50	robert@qa.borderw...	http://newsrss.bbc.co.uk	OCF	Reject
11:17:00	cyril@qa.borderw...	http://www.edenisles.com	Reputati...	Reject
11:16:58	cyril@qa.borderw...	http://www.edenisles.com	Virus -...	Reject
11:14:09	cyril@qa.borderw...	http://www.edenisles.com	Virus -...	Reject
11:14:08	cyril@qa.borderw...	http://www.edenisles.com	Virus -...	Reject
11:14:06	cyril@qa.borderw...	http://www.edenisles.com	Virus -...	Reject
11:00:48	robert@qa.borderw...	http://newsrss.bbc.co.uk	OCF	Reject
10:44:49	cyril@qa.borderw...	http://hakohlae.com	UBL	Reject
10:44:46	cyril@qa.borderw...	http://hakohlae.com	UBL	Reject
10:44:45	cyril@qa.borderw...	http://hakohlae.com	UBL	Reject

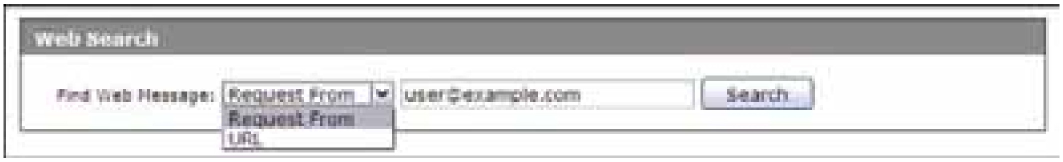
Each web request that passes through the system is given a unique Request ID. Hover over the icon to the left of the request to see the **Request ID** of the web request. Click the icon to see the processing details of the web request.

In the default Web Proxy configuration, only rejected requests or requests that are matched in a content control feature are logged in the *Recent Web Activity* page. To see the activity of all web requests, including those that passed all security and content checks, enable **Verbose Logging** in **Configuration > Web > HTTP/S Proxy** advanced settings.

> **Warning** *The Verbose Logging option should only be enabled for troubleshooting purposes for a short duration of time. Performance is negatively affected when Verbose Logging is enabled and the system processes web requests.*

To search the recent web activity:

1. From the **Find Web Message** drop-down list, select to search on the **Request From** or **URL**.



2. In the **Find Web Message** text box, type a search term that exactly matches the Request From user address or a specific URL.

   For example, `user@example.com` or `www.example.com`.
3. Click **Search**.
   The Message History page appears with the search results.

Status and Actions

These tables describe the different types of messages that can appear in the Status and Action columns on the *Recent Mail Activity* and *Recent Web Activity* pages on the Dashboard

Status	Description
TDR	Message was acted upon by the Threat Prevention feature
Very Malformed	Message was considered very malformed
Invalid Sender EHLO	Message sender does not have a valid sender EHLO
Invalid Sender HELO	Message sender does not have a valid sender HELO
Invalid Sender Domain	Message sender domain does not have a valid DNS A or MX record
Non-FQDN	Message sender is not in correct FQDN (Fully Qualified Domain Name) form
Missing reverse DNS	Message sender does not have a corresponding PTR record for reverse lookups
Unknown sender domain	Message sender domain does not have a valid DNS A or MX record
Missing MX	Message sender domain does not have a valid DNS MX record
Unknown recipient	Message included an unknown recipient
Virus - McAfee	Message was acted upon by McAfee Anti-Virus
Virus - Kaspersky	Message was acted upon by Kaspersky Anti-Virus
PBMF	Message was acted upon by a Pattern Filter

Status	Description
Rules	Message was acted upon by Content/Connection Rules
Malformed	Message was classified as malformed
Threat Outbreak Control	Message was acted upon by the Outbreak Control feature
Mail Access Control	Message was acted upon by Mail Access controls
Attachment Control	Message was acted upon by the Attachment Control feature
OCF	Message was acted upon by the Objectionable Content Filter
Trusted Sender	Message contained a Trusted Sender that bypassed all spam filters
ACS	Message was acted upon by the Content Scanning feature
DFP	Message was acted upon by Document Fingerprinting
SAP	Message was acted upon by a Specific Access Pattern
PostX Encrypt	Message was encrypted by PostX encryption
SecureMail Encrypt	Message was encrypted by SecureMail encryption
Certainly Spam	Message was classified as Certainly Spam by Intercept
Probably Spam	Message was classified as Probably Spam by Intercept
Maybe Spam	Message was classified as Maybe Spam by Intercept
User Spam Train	Message was submitted by a user as Spam
User Not Spam Train	Message was submitted by a user as Not Spam
Brightmail Spam	Message was classified as Brightmail spam
Brightmail Suspected	Message was classified as Brightmail suspected spam
HAM	Message was trained as legitimate mail by Token Analysis
DomainKeys	Message was acted upon by DomainKeys
SPF	Message was acted upon by Sender Policy Framework (SPF)
Reputation Enabled Defense Dialup	Message was classified by Reputation Enabled Defense as a dial-up connection
DNSBL matches above threshold	Message was acted upon by the DNS Block List feature and exceeded the DNS Block List threshold
Reputation above threshold	Message was classified by Reputation Enabled Defense as above the configured reputation threshold
Mail Anomalies	Message was acted upon by the Mail Anomalies feature
Reputation Enabled Defense Infected	Message was considered to be sent from a recently virus-infected source by Reputation Enabled Defense
Relay	Message was relayed to another system

Status	Description
UBL	Message was acted upon by the URL Block List feature (Email or Web)
Clean	Message passed all threat and content checks
Blocked Sender	Message contained senders on a Blocked Sender list
URL Categorization	Web request was acted upon by the URL Categorization feature
HTTP Blocked	Web request was acted upon by the HTTP Blocked Sites list
TLS Failure	Message failed to connect via TLS
TLS Used	Message was delivered via TLS
TLS Refused	Attempt to deliver message via TLS was refused
TLS Not Offered	TLS was not offered when message was delivered
Attachment Size	Attachment size of a message was greater than the size threshold

Action	Description
Discard	The message was discarded without notification to the sender
Quarantined	The message was sent to the administrative quarantine area
Subject Modified	The message subject was modified before it was delivered
Header Added	A message header was added before it was delivered
Reject	The message was rejected with notification to the sender
Temporary Reject	The message was temporarily rejected and the system attempts to deliver the message at a later time
Undeliverable	The message is considered permanently undeliverable after multiple attempts to deliver the message
Bounce	The message has been bounced back to the sender by the destination mail server and is permanently undeliverable
Incomplete	The SMTP connection to deliver the message was not completed
Failed	The attempted message delivery failed
Release	The message was released from the quarantine
Relay	The message has been relayed to another system
Soft Bounce	The message was bounced back by the destination mail server before it reached the intended recipient
Sent	The message has been sent but there is not yet confirmation of its delivery

Action	Description
Forwarded	The message has been forwarded to another recipient
Deferred	The message delivery is deferred and is retried at a later time
Delayed	The message delivery is delayed and is retried at a later time
Redirect	The message has been redirected to another system, for example, a quarantine or encryption server
BCC	A Blind Carbon Copy was created for the message and sent to the BCC contact
Bypass	The message bypassed all spam and content controls
PostX Encrypt	The message was encrypted by the integrated PostX encryption engine
SecureMail Encrypt	The message was encrypted by the integrated SecureMail encryption engine
Trust	The message was considered trusted for scanning purposes
Accept	The message was accepted for scanning and delivery
Archive Copy	The message was copied to an archive server
Pass	The message passed all threat and content scanners and was delivered to its destination
Do Not Train	The message is not used as training for Token Analysis
Not Trained	The message was not used as training for Token Analysis
Trained	The message was used for training by Token Analysis
Just Log	The action on the message was only sent to the log files, and the message delivered to its destination

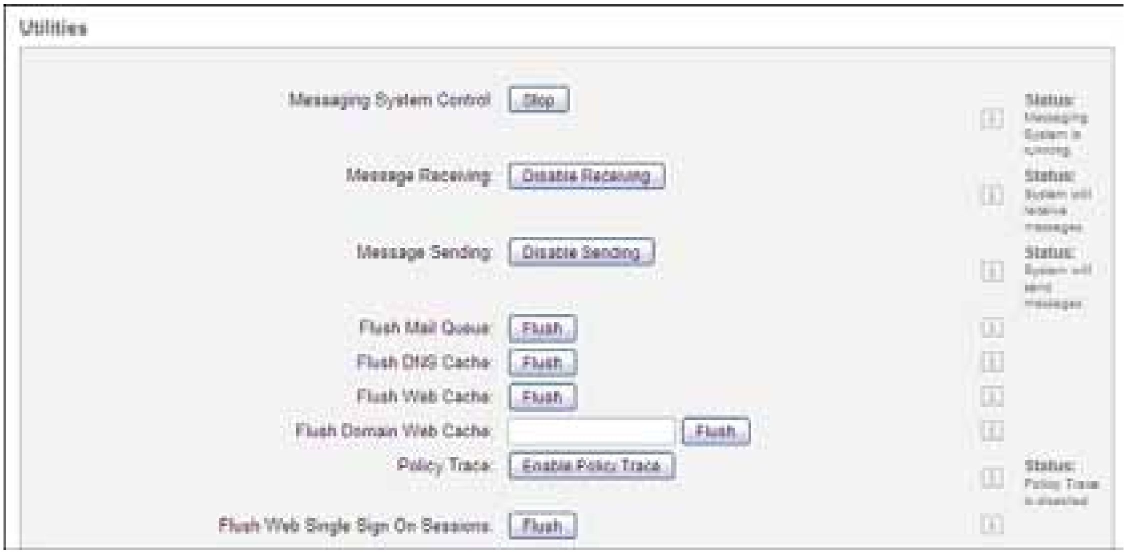
System Utilities

The *Utilities* page (**Activity > Status > Utilities**) provides the following utilities:

- Controls to start and stop the message processing
- Flush the mail queues, DNS cache, and Web cache
- Policy trace
- Diagnostic tools, for example, a Hostname Lookup function, SMTP Probe, Ping, and Traceroute utilities that are useful to resolve message and network problems.

Messaging System Controls

You can control the flow of message processing for inbound and outbound messages.



Status: Messaging System is running

Status: System will receive messages

Status: System will send messages

Status: Policy Trace is disabled

- **Messaging System Control**– To stop or start all email and web messaging services, click on the **Stop** or **Start** Messaging System Control button.

> ***Warning*** *The Stop and Start messaging controls are replicated in a cluster environment. When you stop message processing on the Primary, you stop message processing on all devices in the cluster.*

- **Message Receiving** – You can enable or disable only the receiving of messages when you click the **Disable Receiving** or **Enable Receiving** button. This is useful if you only want to stop the processing of inbound messages. For example, you may want to turn off the receiving of messages to troubleshoot errors with inbound mail, but still send outbound messages.
- **Message Sending** – You can enable or disable only the sending of messages when you click the **Disable Sending** or **Enable Sending** button. This is useful if you only want to stop the processing of outbound messages. For example, you may want to turn off the sending of messages to troubleshoot errors with SMTP delivery, but still receive inbound messages.

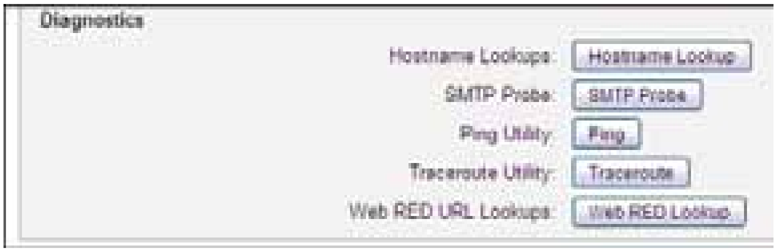
Utilities

- **Flush Mail Queue** – The **Flush** button is used to reprocess any queued mail in the system. Only click this button once. If the mail queue does not process, you may have other types of delivery problems, and additional flushes only add more load on your XCS device.
- **Flush DNS Cache** – Click **Flush** to remove all entries from the current DNS cache. Use this option to clear the entries in the DNS cache if you cannot resolve host names because of cached DNS queries.
- **Flush Web Cache** – Click **Flush** to manually purge the HTTP Proxy web disk cache. Administrators may want to purge the entire web cache if there are issues with certain web pages that do not update with newer content, or issues when you connect to specific web sites.
- **Flush Domain Web Cache** – You can flush the Web Cache for a specific domain only. The URL must be specified exactly the way it is typed, for example, *www.example.com*, or *news.example.com*. Subdomains are not included and they must be separately flushed. When the domain has been entered, click **Flush**.

- **Policy Trace** – Click **Enable Policy Trace** to enable more detailed log messages for policy resolution in the messaging logs.
- **Flush Web Single Sign-on Sessions** – Flushes all Web Proxy authenticated single sign-on sessions for both Proxy and Portal IP address-based authenticated users. Current Web Proxy users must re-authenticate before they can get access through the Web Proxy.

Diagnostics

The *Diagnostics* section contains networking and SMTP utilities to help troubleshoot network and message delivery issues.



- **Hostname Lookup** – Verifies host name resolution with a query to a DNS name server.
- **SMTP Probe** – Sends a test email to a remote SMTP server.
- **Ping** – Test network connectivity with ICMP ping.
- **Traceroute** – Traces the routes of network data from the source to the destination server to test connectivity.
- **Web RED URL Lookups** – Lookup the web reputation of a specific URL.

Mail Queue

The *Mail Queue* page contains information on mail waiting to be delivered. Mail may be deferred because the destination mail system cannot be contacted.

If a message is deferred, this schedule is used to try another mail delivery:

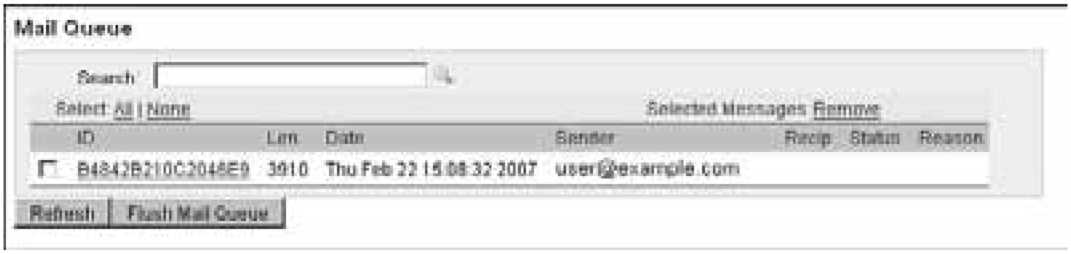
- 1000 seconds (first retry)
- 2000 seconds (second retry)
- 4000 seconds (third and subsequent retries until the message is delivered or the message expires in the queue)

> ***Note*** *The Maximum Time in Mail Queue setting is configured via* ***Configuration > Mail > Delivery****.*
> *The default is 5 days. You can enable mail queue monitoring in the advanced settings.*

To see and manage the mail queue:

1. Select **Activity > Queue/Quarantine > Mail Queue**.
2. You can take these actions:
   - Use the **Search** field to search for a specific mail message.
   - To remove undeliverable messages, select the message and click **Remove**.
   - Select **Remove All** to remove all messages in the queue.

- To process messages out of the queue, click **Flush Mail Queue**. Only click this button once. If the mail queue does not process, you may have other types of delivery problems and reprocessing the mail queue only adds additional load to the system.



	ID	Len	Date	Sender	Recip	Status	Reason
□	B4842B210C2046E9	3910	Thu Feb 22 15:08:32 2007	user@example.com			

Display Options

You can append these options to the URL of the Mail Queue page:

- **?limit=n** — Sets the total number of mail queue items in the list. The default is 2000.
- **?ipp=n** — Sets the number of items per page.
- **?order=asc** — Sorts items by oldest date first to the most recent.

For example, to set the total number of displayed items to 100, use this URL:

```
https://hostname.example.com/ADMIN/mailqueue.spl?limit=100
```

Use the “&" symbol instead if an “?” option already exists:

```
https://hostname.example.com/ADMIN/mailqueue.spl?action=submit&limit=100
```

Message Quarantine

The *Message Quarantine* contains messages that have been quarantined because of a virus, malformed message, content violation, an illegal attachment, or attachments over the size limit.

To see and manage the message quarantine:

1. Select **Activity > Queue/Quarantine > Message Quarantine**.
2. You can take these actions:
   - Click a **Message ID** number to see the message details
   - Click **Delete** to delete the message from the quarantine
   - Click **Release** to release messages from the quarantine and deliver them to their original destination

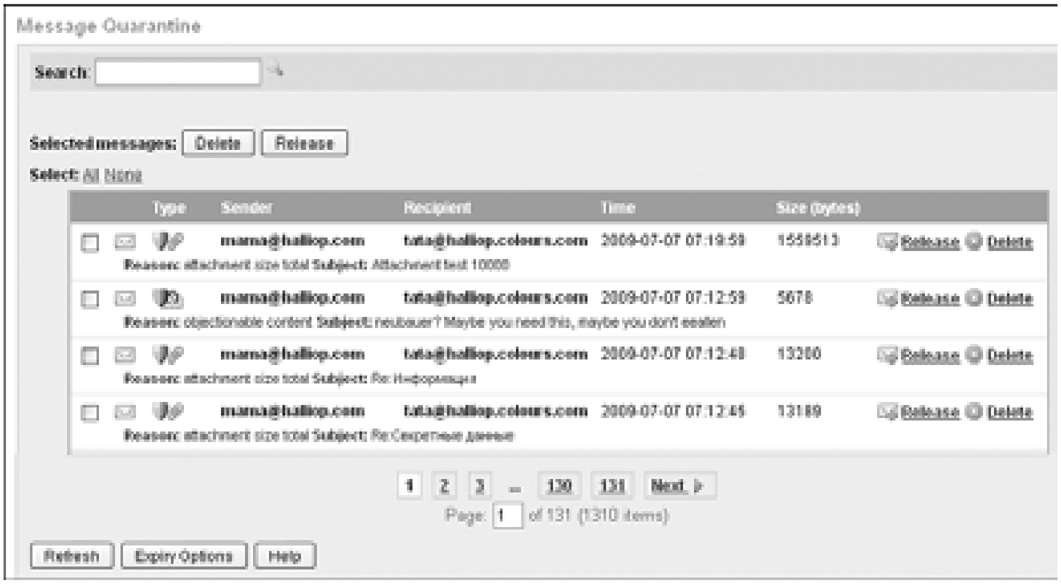
> ***Note*** *The Delete All and Release All buttons are used specifically with the search function. You must enter a specific search pattern before you use these controls. We recommend that you use the Expiry Options button to clear the quarantine area of all messages beyond a certain date.*

3. Use the **Search** field to look for specific messages in the quarantine.

   For example, you could search for the name of a specific virus so that any quarantined messages infected with that specific virus are displayed.

   You can search these message fields:

- Sender, Recipient, or QueueID
- Type (for example, *attachment*, *attachment size*, *malformed*, *virus*, *spyware*, *objectionable*, *compliance*, *antispam*, *pbmf*, *content rules*, *dfp*, or *possible virus* to restrict the search to those types of messages.). You can combine the specified message type and include an attachment, virus, or spyware name, for example, `attachment file.exe`)
- Date and time (for example, 2009-09-14, 20:27:34, or both 2009-09-14 20:27:34)
- Filename
- Virus or spyware name
- File Size



Message Quarantine

Search:

Selected messages: Delete Release

Select: All None

	Type	Sender	Recipient	Time	Size (bytes)	
□		mama@halliop.com	tata@halliop.colours.com	2009-07-07 07:19:59	1559513	Release Delete
Reason: attachment size total Subject: Attachment test 10000						
□		mama@halliop.com	tata@halliop.colours.com	2009-07-07 07:12:59	5678	Release Delete
Reason: objectionable content Subject: neubauer? Maybe you need this, maybe you don't esalen						
□		mama@halliop.com	tata@halliop.colours.com	2009-07-07 07:12:48	13200	Release Delete
Reason: attachment size total Subject: Re: Информация						
□		mama@halliop.com	tata@halliop.colours.com	2009-07-07 07:12:45	13189	Release Delete
Reason: attachment size total Subject: Re:Секретные данные						

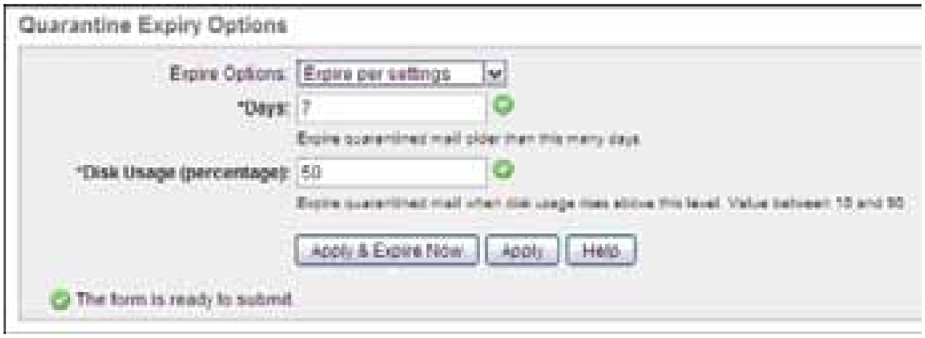
Page: 1 of 131 (1310 items)

Quarantine Expiry Options

You can set an expiration term so that quarantined messages are deleted after a certain period of time. You can use this feature to flush all messages from the quarantine area on a regular basis.

To set the expiry options:

1. Click **Expiry Options**.



Quarantine Expiry Options

Expire Options: Expire per settings

*Days: 7

Expire quarantined mail older than this many days

*Disk Usage (percentage): 50

Expire quarantined mail when disk usage rises above this level. Value between 10 and 90

The form is ready to submit.

2. Choose the **Expire Options** mode:

- **Expire only on disk full** – The Quarantine expires messages from the quarantine when the disk is 90% full.
- **Expire per settings** – The Quarantine expires messages based on the settings configured by the administrator.
- **Days** – Enter how many days to keep a quarantined message before it is deleted.
- **Disk usage (percentage)**– Enter a percentage of disk usage that is used by the quarantine storage area. Valid values are between 10% and 90%. The disk partition used by the quarantine is the *System Data Storage Area* partition. If the usage for this disk partition grows beyond the specified size, messages are expired, starting with the oldest message, until the percentage is below the limit.

> **Note** *The Delete All and Release All buttons are used specifically with the search function. You must enter a specific search pattern before you use these controls. We recommend that you use the Expiry Options button to clear the quarantine area of all messages beyond a certain date.*

3. Click **Apply** to apply these settings for new quarantined messages, or click **Apply and Expire Now** to apply these settings and expire currently quarantined messages immediately.

Message History

Every message that passes through the system generates a database entry that records information about how it was processed, filtered, and delivered. To see how the message was processed, you can examine the message history database to see the disposition of the message.

Messages are searched and displayed based on the type of message (email and web) and the message part. For example, you can search for partial or specific text in the subject header of all email messages in the database.

To see the message history:

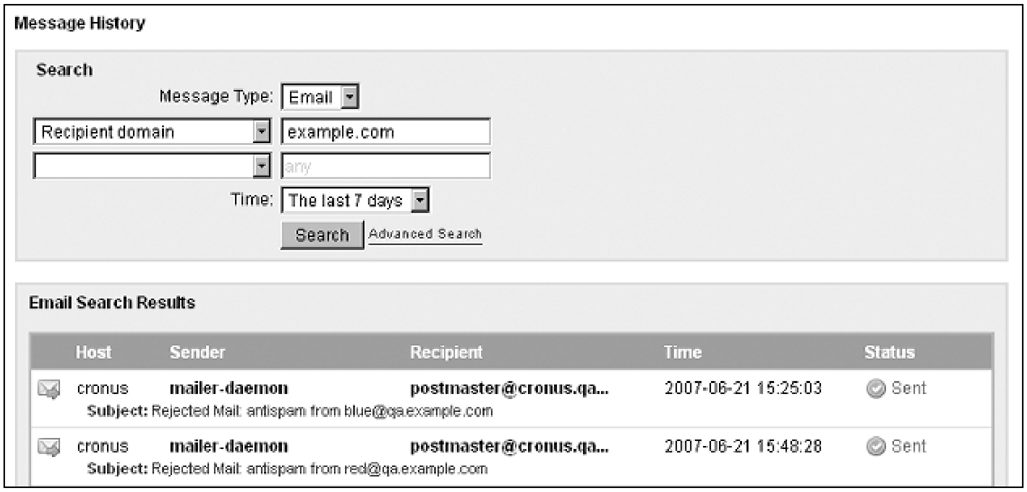
1. Select **Activity > History > Message History**.
2. Examine the **Status** column for full information on how a message was processed and its final disposition.
3. Use the search fields to filter the message history results.

   All simple search fields default to exact matches, except for *Subject*, which accepts partial matches, and *Domain part*, which matches the ending of a domain part. For more detailed and flexible searches, use the **Advanced Search** option.

   > **Note** *A maximum of 100,000 search results are displayed. Use the search parameters to narrow your search and improve the search results. See Message History for more details.*

   You can also take these actions:

   - Click the **Download these results** link to save the search results as a local file. You can search this file offline for more efficient results.
   - Click on a **Message ID** to see the details of the message.
   - Click **Show Log** to see the corresponding log entry for this message.



Message History

Search

Message Type: Email

Recipient domain: example.com

any

Time: The last 7 days

Email Search Results

Host	Sender	Recipient	Time	Status
cronus	mailer-daemon	postmaster@cronus.qa...	2007-06-21 15:25:03	Sent
Subject: Rejected Mail: antispam from blue@qa.example.com				
cronus	mailer-daemon	postmaster@cronus.qa...	2007-06-21 15:48:28	Sent
Subject: Rejected Mail: antispam from red@qa.example.com				

Email History Search

You can search for email messages with these message fields:

- **FROM/Sender** – When you search on FROM/Sender, it includes these message fields:
- **Envelope Address** – The Envelope From address in the SMTP envelope.
- **Header Address** – The From address in the message header.
- **TO/CC/BCC/Recipients** – When you search on TO/CC/BCC/Recipients, it includes these message fields:
- **Account/Mailbox Part** (for example, `user1` in the email address `user1@example.com`)
- **Domain Part** (for example, `example.com`)
- **Subject** – Searches the subject field of a message. The subject field search additionally checks for variations on the subject specified in any part of the subject. For example, if you search on `spam message`, the system matches on `spam message`, `message spam`, `this message is spam` and also plurals, for example, `spam messages`.
- **SMTP HELO message** – Searches on text in the SMTP HELO message that identifies the SMTP client to the server.
- **Client IP** – Searches on the client IP address, for example, `10.0.1.100`.
- **Client Host** – Searches on the client hostname, for example, `hostname` in the fully qualified domain name `hostname.example.com`.
- **Message ID** – Searches on the Message ID that is added by a mail server, for example, `8290352619373D0@server.example.com`.
- **Queue ID** – Searches on the Queue ID of a message, for example, `CE9D0C23183D8E2B`.
- **Prior Queue ID**– Searches on the prior Queue ID of a message. If a message is forwarded because of alias expansion, vacation notification, or because it was bounced, a new message is created in the queue.
- **Virus** – Searches for messages that contained a specific virus.
- **Spyware** – Searches for messages that contained a specific type of spyware.
- **Attachment Type** – Searches messages for specific attachment types.
- **Authentication** – Searches messages based on their SMTP authentication status.

HTTP History Search

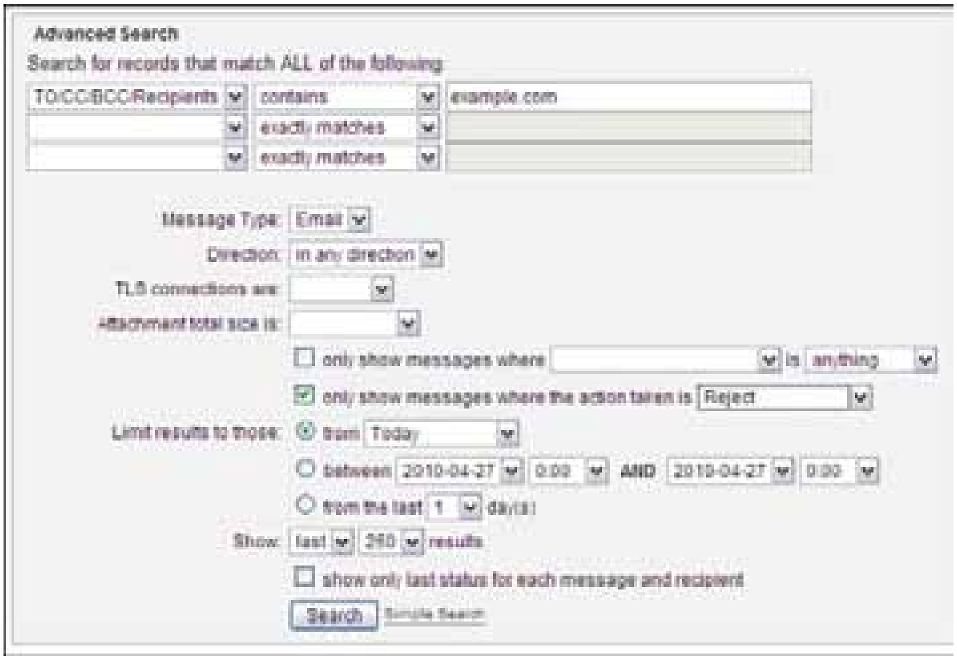
You can search for web requests and sessions with these fields:

> ***Note*** *There are no message details for successful web sessions. The browse time for successful sessions is indicated in the status column of the search results.*

- **Client IP** – Searches web requests and sessions based on the IP address of the web client, for example, `10.0.1.100`.
- **Request ID** – Searches on the Request ID added to the request by the system, for example, `8290352619373D0`. This field can also be used to search web sessions.
- **URL** – Searches on the URL of the HTTP request, for example, `www.example.com`. This field can also be used to search web sessions.
- **Request From** – Searches on the user name of the originating client request if authentication is enabled for the Web Proxy. If authentication is not enabled, use the **Client IP** option to search requests for specific client IP addresses. This field can also be used to search web sessions.
- **Virus** – Searches for messages that contain the specified virus.
- **Spyware** – Searches for messages that contain the specified spyware name.
- **Attachment Type** – Searches on the attachment type of any attachments filtered by the Attachment Control and Content Scanning features. The specified search term must match the Content-type for the attachment, as displayed in the HTTP log. For example, to match a .exe attachment, you must enter a partial or exact search on the Content-Type name of `application/x-msdos-program`.

Advanced Search

Click the **Advanced Search** link to expand the number of options to use to search the database. The advanced search includes additional parameters, for example, advanced date ranges, message direction, TLS status, and the final action taken on messages.



Advanced Search

Search for records that match ALL of the following

TO/CC/BCC/Recipients | contains | example.com
| exactly matches |
| exactly matches |

Message Type: Email

Direction: in any direction

TLS connections are:

Attachment total size is:

☐ only show messages where [ ] is anything

☑ only show messages where the action taken is Reject

Limit results to those: ● from Today

○ between 2010-04-27 0:00 AND 2010-04-27 0:00

○ from the last 1 day(s)

Show: last 250 results

☐ show only last status for each message and recipient

Message History Search Tips

The message history search methods have been optimized to work most efficiently when used to locate messages using specific criteria in a narrow time period. Try to narrow your searches to the smallest time period possible, and avoid searches for all time periods (Anytime). This is especially important for systems that process a large volume of messages,. The most efficient way to retrieve results is to narrow your search to a single daily time period.

On the **Simple Search** page, the default search criteria option is **exactly matches** (case sensitive) for all search items except for these fields:

- **Subject** – Defaults to **contains**. Subject searches with the **contains option** use substring matching. Use the **contains keywords** option for full text search of subject fields for fast searches of space-delimited languages.
- **Recipient Domain Part** – Defaults to **ends with**.

For all other search items, the **contains** option is the least-efficient possible search method. If possible, narrow your search using the options **exactly matches**, **starts with** or **ends with,** which are more efficient for message searches. For more detailed and flexible searches, use the **Advanced Search** page.

Specify these search fields in your query for the most efficient searches:

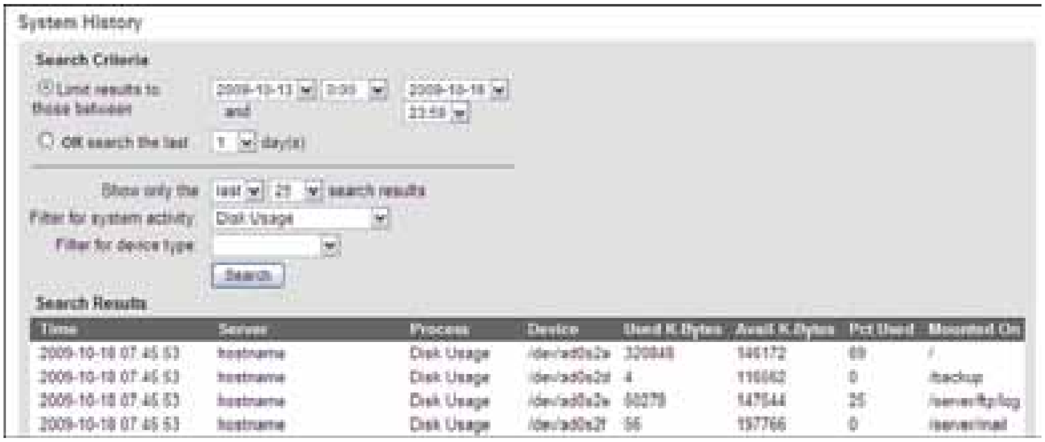
- Queue ID
- Sender Envelope Address
- Sender Header Address
- Sender Display Name
- Recipient Account/Mailbox Part
- Recipient Domain Part
- Subject

System History

The *System History* is a record of system-related information and events, for example, processes, message queue sizes, administrative and log in activity, network/disk space use, swap file, and disk paging statistics.

To get access to the system history:

1. Select **Activity > History > System History**.



System History

Search Criteria

● Limit results to those between 2009-10-13 0:00 and 2009-10-18 23:59

○ OR search the last 1 day(s)

Show only the last 25 search results

Filter for system activity: Disk Usage

Filter for device type:

Search Results

Time	Server	Process	Device	Used K Bytes	Avail K Bytes	Pct Used	Mounted On
2009-10-18 07:45:53	hostname	Disk Usage	/dev/ad0s2a	320848	146172	69	/
2009-10-18 07:45:53	hostname	Disk Usage	/dev/ad0s2d	4	116582	0	/backup
2009-10-18 07:45:53	hostname	Disk Usage	/dev/ad0s2e	60279	147544	25	/server/ftp/log
2009-10-18 07:45:53	hostname	Disk Usage	/dev/ad0s2f	56	157766	0	/server/mail

2. Set the **Search Criteria** to restrict the search to a specific range of dates or number of days.
3. Click **Search**.

   Search results are filtered based on the type of system activity/process, or a specific hardware device.

   This table provides a description of the search fields.

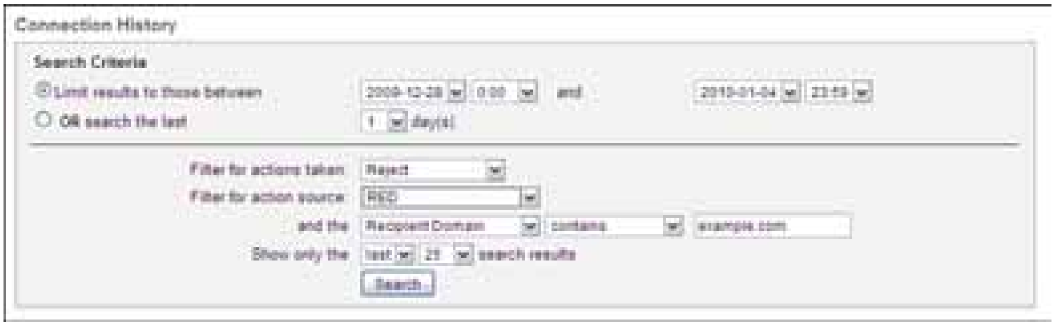
System Activity	Description
Admin Actions	Displays a list of actions taken by an administrative user. This includes commands and logins.
Avg. Waiting Processes	The average number of waiting CPU processes for the past 1, 5, and 15 minutes.
DNS Lookup Performance	Displays performance information for DNS lookups.
Disk Loading (Other)	Displays the MB per second, KB per transfer, and transfer per second, for each non-SCSI disk.
Disk Loading (SCSI)	Displays the MB per second, KB per transfer, and transfer per second, for each SCSI disk.
Disk Usage	Amount (in KB) of used disk space, total available disk space, and percentage used for each disk slice.
Disk Usage Inodes	Amount of used inodes, available inodes, and percentage inodes used for each disk slice.
Login Failures	Displays information on failed web admin or WebMail logins to the system.
Login Success	Displays information on successful web admin or WebMail logins to the system.
Logout	Displays information on web admin or WebMail logouts from the system.
Logout Expiry	Displays information on logins that expired and were automatically logged out of the system.
Network Usage	Amount of data inbound and outbound (in bytes) on the network interface.
Paging	The number of disk pages in and out.
Pattern File Download	Status of Anti-Virus pattern file downloads.
Queue size	Amount of mail waiting in the Mail or Deferred Queue.
Swap	Used and available swap space in megabytes.

Connection History

The *Connection History* is a log history of connections to the system from other systems. The history shows the time of the connection, the server name and IP address, the action taken on the connection and its source, properties (trusted or untrusted), and the reject details if the message was rejected.

To see the connection history:

1. Select **Activity > History > Connection History**.



Connection History

Search Criteria

● Limit results to those between 2009-12-28 0:00 and 2010-01-04 23:59

○ OR search the last 1 day(s)

Filter for actions taken: Reject

Filter for action source: RED

and the: Recipient Domain, contains, example.com

Show only the: last 25 search results

2. Set the **Search Criteria** to restrict the search to a specific range of dates or number of days.
3. Click **Search**.

   Search results are filtered based on the actions taken on that connection and the action source, for example, a connection refused because of a low reputation score by Reputation Enabled Defense.

   This table provides a description of the search fields.

> ***Note*** *The Sender and Recipient fields are empty for connections that are rejected before that information is received, for example, in the case of an IP address that was blocked.*

Action	Description
Accept	Connection passed the initial connection checks and was accepted by the system.
Just Log	Connection and its processing was recorded in the log file only.
Pass	Connection was accepted by the system and the messages passed all content and security checks.
Reject	Connection was rejected with notification to the connecting system.
Relay	Connection was relayed through this system.
Temporary Reject	Connection was temporarily rejected. The connection is retried at a later time.

Source	Description
Reputation Dialup	Connection was detected as a dialup source by the Reputation Enabled Defense service.
Reputation Infected	Connection was considered to be a source of virus infections by the Reputation Enabled Defense service.
RED	The connection’s Reputation Enabled Defense reputation score exceeded the reputation reject threshold.

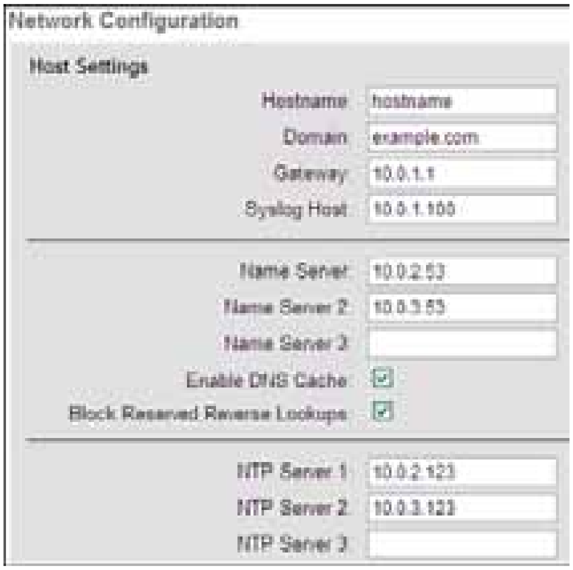
Source	Description
Blocked Sender	Sender of a message in the connection was on the Blocked Senders List.
Clean	Connection was allowed and messages were processed as clean.
DNSBL matches above threshold	Connection was rejected by a DNS Block List because the number of DNSBL matches exceeded the threshold.
Invalid Sender Domain	Connection contained an invalid sender domain address.
Mail Access Control	Connection violated a threshold in the Mail Access settings (for example, message too large).
PBMF	Connection matched a Pattern Filter rule.
Relay	Connection was allowed to Relay through this system.
SAP	Connection matched a Specific Access Pattern.
TDR	Connection was acted on by the Threat Prevention feature.
Trusted Sender	Sender of a message in the connection was on a Trusted Senders List.
UBL	Connection (Email or Web) contained a URL that matched on a URL Block List.
Very Malformed	Connection contained very malformed messages.
Rule Match	Connection information was matched in a Connection Rule.

Syslog Host

You can forward all of the system's log files to a syslog server, which is a computer that collects and stores log files from many sources. The syslog files can then be analyzed by a separate logging and reporting program.

To define a syslog host:

1. Select **Configuration > Network > Interfaces**.
2. In the **Host Settings** section, type the address of the syslog server in the **Syslog Host** field.



Network Configuration

Host Settings

Hostname	hostname
Domain	example.com
Gateway	10.0.1.1
Syslog Host	10.0.1.100
Name Server	10.0.2.53
Name Server 2	10.0.3.53
Name Server 3	
Enable DNS Cache	☑
Block Reserved Reverse Lookups	☑
NTP Server 1	10.0.2.123
NTP Server 2	10.0.3.123
NTP Server 3	

3. Click **Apply**.

SNMP (Simple Network Management Protocol)

Simple Network Management Protocol (SNMP) is the standard protocol for network management. When enabled on the WatchGuard XCS, this feature gives standard SNMP monitoring tools the ability to connect to the SNMP agent that runs on the XCS system and extract real-time system information.

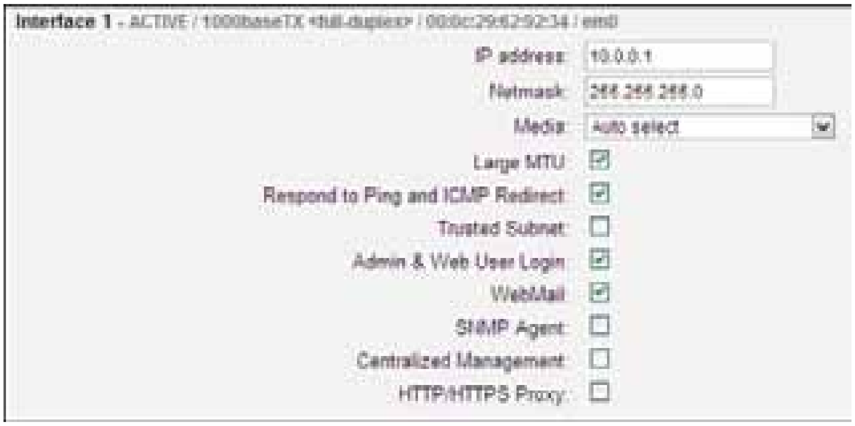
The information available from the SNMP agent is organized into objects that are described by the MIB (Management Information Base) files. The information available includes disk, memory, and CPU statistics, mail queue information, and statistics on the number of spam or virus-infected emails. An SNMP trap is sent when the system reboots.

Note *The SNMP MIB files are based on SNMP version 2 and are backwards compatible with version 1.*

The SNMP agent service is installed and running by default, but it must be enabled specifically to monitor a network interface as required.

To add SNMP access to a network interface:

1. Select **Configuration > Network > Interfaces**.
2. Select the **SNMP Agent** check box on the required interface.
   We strongly recommend that the agent only be configured for the internal (trusted) network.



Interface 1 - ACTIVE / 1000baseTX <full-duplex> / 00:0c:29:62:92:34 / em0

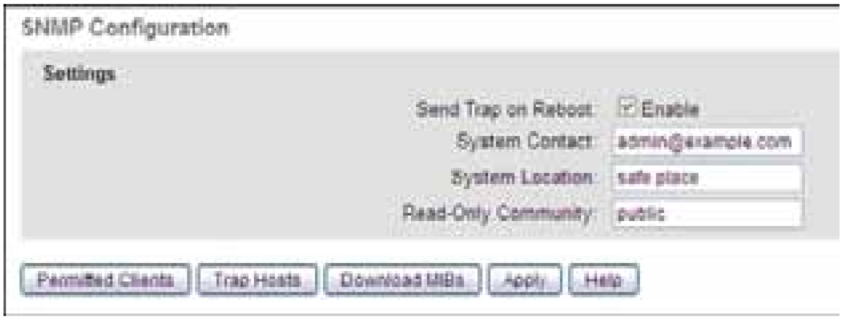
IP address: 10.0.0.1
Netmask: 255.255.255.0
Media: Auto select
Large MTU: ☑
Respond to Ping and ICMP Redirect: ☑
Trusted Subnet: □
Admin & Web User Login: ☑
WebMail: ☑
SNMP Agent: □
Centralized Management: □
HTTP/HTTPS Proxy: □

3. Click **Apply**.
   You must restart the device.

Configure SNMP

To configure SNMP:

1. Select **Configuration > Network > SNMP**.



SNMP Configuration

Settings

Send Trap on Reboot: ☑ Enable
System Contact: admin@example.com
System Location: safe place
Read-Only Community: public

2. Select the **Send Trap on Reboot** check box to send a trap message to your SNMP trap host when the system reboots.
   A trap is sent when the system shuts down, and another trap is sent when the system restarts.
3. Enter the email address of the **System Contact** for this device.
4. Enter the **System Location** for this device.
5. Enter the **Read-Only Community** string (case-sensitive) for this device.

   By default, the system does not allow read/write access to the SNMP agent. For read access, you must set up a read-only community string on both the agent and your SNMP management application for authentication. We recommend that you change the default community string “public” to a more secure value.

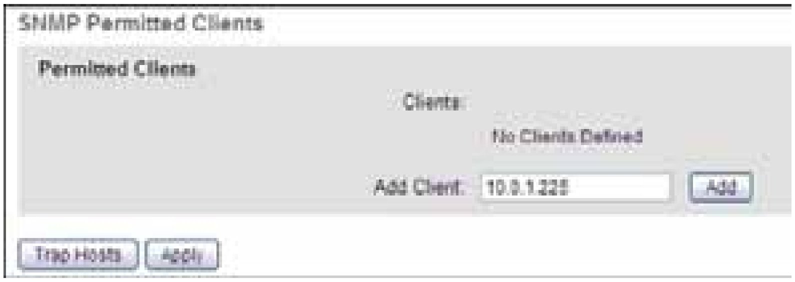
6. Click **Apply**.

Permitted Clients

To enable access to the system’s SNMP agent, you must specifically add the client system to the list of SNMP permitted clients.

To add permitted clients:

1. Enter the address of your SNMP management station.
   The clients are specified with a host name, IP address, or CIDR network address (192.168.128.0/24).
2. Click **Add** to add the permitted client.
3. Click **Apply**.

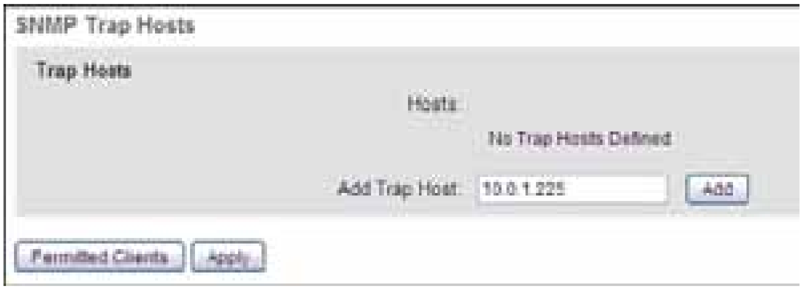


Trap Hosts

A trap host is an SNMP management station that receives system traps from the WatchGuard XCS. The system sends an SNMP trap when the system is shut down or restarts.

To add trap hosts:

1. Enter a list of hosts that receive trap messages.
   The hosts are specified with a host name or IP address.
2. Click **Add** to add the trap host.
3. Click **Apply**.



MIB Files

To download the SNMP MIB files, click **Download MIBs**. You must import these files to your SNMP management program. The MIB file contains a list of objects that represent the information that is extracted from the XCS SNMP agent.

Alarms

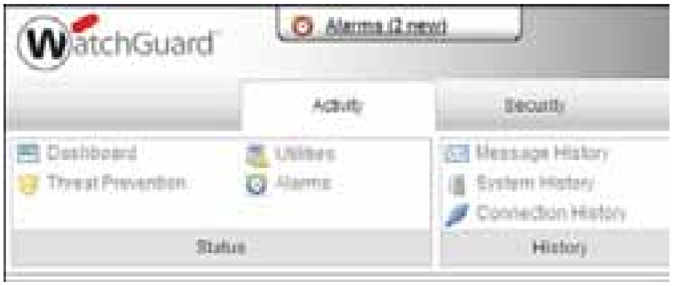
The WatchGuard XCS implements a variety of system alarms to notify the administrator of exceptional system conditions. Alarms are generated from the Queue Replication, LDAP, DNS Intercept queries, and Backup subsystems. For example, you can receive an alarm notification if the daily FTP backup fails, or if queue replication fails. Errors with LDAP user imports also trigger an alarm.

You can select the type of alarm notifications to receive, for example, *Critical*, *Serious*, and *Warning* events.

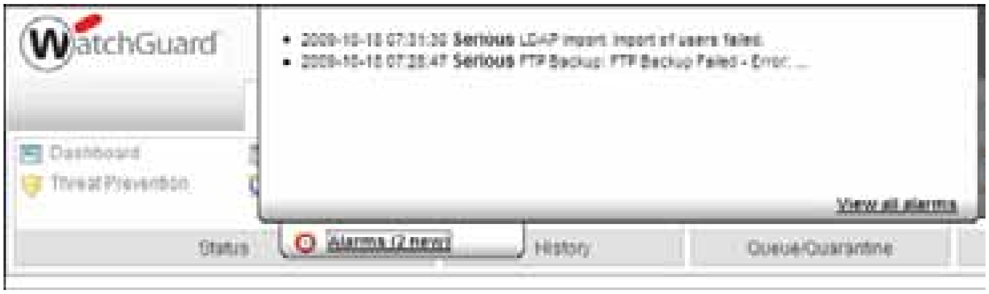
The notifications are sent with these methods:

- Alarms Indicator
- Email notification
- Console Alert

This example shows the **Alarms Indicator** that appear on the administrative user interface page.

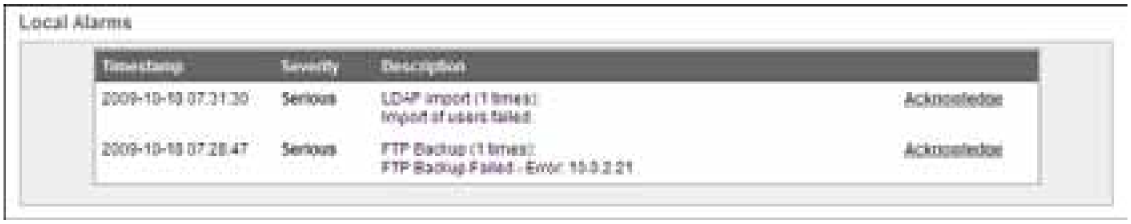


The indicator displays how many new alarms have occurred. Click the **Alarms Indicator** to see a summary of the most recent alarms.



- 2009-10-18 07:31:30 **Serious** LDAP import: Import of users failed.
- 2009-10-18 07:28:47 **Serious** FTP Backup: FTP Backup Failed - Error: ...

Click **View all alarms** in the alarms indicator, or select **Activity > Status > Alarms** to go to the local alarms page where you can see and acknowledge all alarms.



Local Alarms

Timestamp	Severity	Description	
2009-10-18 07:31:30	Serious	LDAP import (1 times): Import of users failed.	Acknowledge
2009-10-18 07:28:47	Serious	FTP Backup (1 times): FTP Backup Failed - Error: 10.0.2.21	Acknowledge

You must click **Acknowledge** to remove the alarm notification.

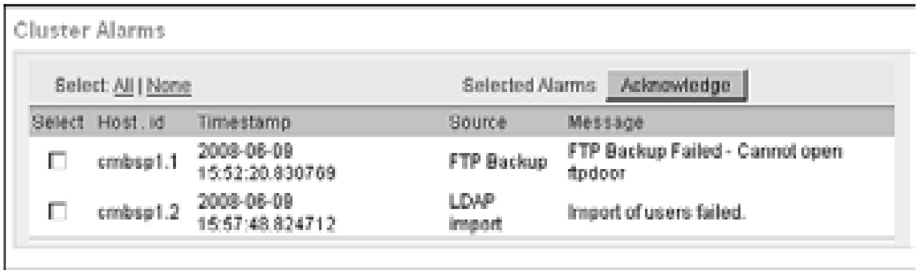
> ***Note*** *Tiered administrators only have a read-only view of the Alarms indicator if the "View Alarms" permission is assigned. Tiered admins can see alarms, but they cannot acknowledge an alarm. Delegated Domain administrators do not have access to the alarms.*

Alarms in a Cluster

You can see and acknowledge local alarms on each individual system in the cluster (Primary, Secondary, or Client). The alarms indicator on any cluster system only shows local alarms for the specific system, and acknowledgement of a local alarm does not clear its status for the cluster.

Alarms generated by the cluster are only available on the Cluster Primary system at **Activity > Status > Cluster Alarms**. The *Cluster Alarms* page indicates alarms that appear on individual systems in the cluster and you can see and acknowledge them on the Primary system. The alarm indicates the specific host in the cluster from where the alarm generated.

> ***Note*** *In certain cases, a cluster alarm appears on a Primary, Secondary, and Client. The alarms must be acknowledged on all systems before the cluster alarm is cleared on the Primary.*



Cluster Alarms

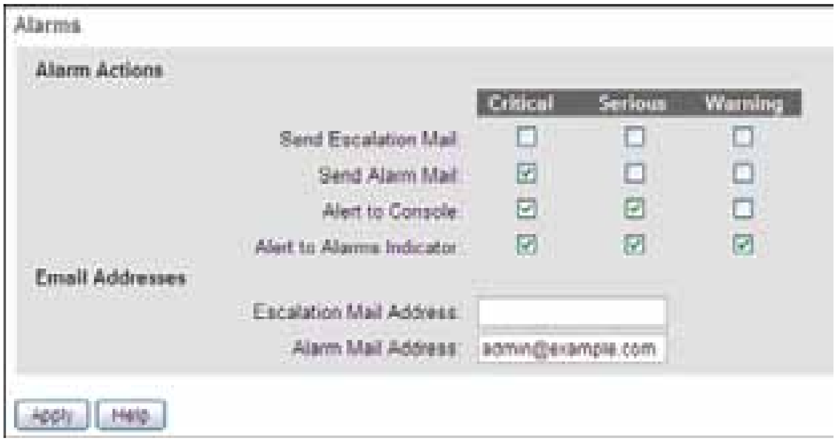
Select: All | None Selected Alarms

Select	Host . id	Timestamp	Source	Message
□	cmbsp1.1	2008-06-09 15:52:20.830769	FTP Backup	FTP Backup Failed - Cannot open ftpdoor
□	cmbsp1.2	2008-06-09 15:57:48.824712	LDAP import	Import of users failed.

Configure Alarms

To configure alarms and notifications:

1. Select **Configuration > Miscellaneous > Alarms**.



Alarms

Alarm Actions

	Critical	Serious	Warning
Send Escalation Mail	□	□	□
Send Alarm Mail	☑	□	□
Alert to Console	☑	☑	□
Alert to Alarms Indicator	☑	☑	☑

Email Addresses

Escalation Mail Address:

Alarm Mail Address: admin@example.com

2. In the **Send Escalation Mail** section, select the types of alarms that send an email to the specified **Escalation Mail Address**.

3. In the **Send Alarm Mail** section, select the types of alarms that send and email to the specified **Alarm Mail Address**.
   The alarm only triggers once for a specific alarm. You do not receive another email alert for the alarm unless you acknowledge the alarm on the Dashboard and it occurs again.

> ***Note*** *You must have a valid address specified in the Email Addresses section for the alarm email notification to be sent.*

4. In the **Alert to Console** section, select the types of alarms that display an alert on the system console screen.
5. In the **Alert to Alarms Indicator** section, select the types of alarms that display an alert on the main administrative user interface page in the alarms indicator.
6. Type the **Escalation Mail Address** to send escalation messages to.
7. Type an **Alarm Mail Address** to send alarm messages to.

> ***Note*** *You should use SNMP for monitoring of system resources, for example, disk space and memory usage. See SNMP (Simple Network Management Protocol) for more information.*

Alarms List

This table describes the types of alarms that can occur.

Severity	Alarm
Critical	LDAP Lookup: LDAP lookup failed during delivery
Critical	LDAP Lookup: LDAP lookup: Unable to bind to server
Critical	LDAP Lookup: LDAP lookup: Search error 81: Can't contact LDAP server
Critical	Queue Replication: Cannot connect to mirror
Critical	kav_pattern_update: No available update servers
Critical	Deferred mail queue threshold exceeded.
Critical	QueueMonitor: Incoming queue size exceeded the “Significant” limit. SMTPDs reject new requests temporarily.
Serious	QueueMonitor: Incoming queue size exceeded the “Medium” limit. The system significantly increases priority of mail delivery over mail receiving.
Critical	Restore: Finished: (indicates if restore successfully PASSED)
Serious	DNS status check (DNSBL, UBL, Reputation)
Serious	Restore: Reporting: Finished: (indicates if reporting restore was completed)
Serious	FTP Backup: FTP Backup Failed
Serious	SFTP Backup: SFTP Backup Failed
Serious	SCP Backup: SCP Backup Failed

Severity	Alarm
Serious	LDAP Import: LDAP import, Import of groups failed
Serious	LDAP Import: LDAP import, Import of users failed
Serious	LDAP Import: LDAP failed to download users, groups
Serious	mxlogging: could not rollover/offload some files. Please see details in Systems Log (messages).
Serious	mxlogging: [error message]
Warning	QueueMonitor: Incoming queue size exceeded the “Minor” limit. The system slightly increases the priority of mail delivery over mail receiving.

22 Troubleshooting

Troubleshoot Message Delivery

When message delivery problems occur, the first step to troubleshoot the issue is to examine if the problem is affecting only incoming messages, outgoing, or both. For example, if you receive messages, but cannot send outgoing messages, it is certain that your Internet connection is working properly, or you would not be able to receive messages. In this scenario, you may have issues with a network firewall blocking your outbound connections, or some other issue that prevents message delivery.

Problems that affect both inbound and outbound delivery include these scenarios:

- **Network Infrastructure and Communications** – The most common scenario in which you cannot send or receive messages is if your Internet connection is down. This can include upstream communications with your ISP, your connection to the Internet, or your external router. You must also check your internal network infrastructure to make sure you can contact the WatchGuard XCS from your router or firewall.
- **DNS** – If your DNS is not working or configured properly, messages are not forwarded to your WatchGuard XCS and you cannot lookup external messaging or web servers. Make sure the DNS service is running, and check your DNS records for any misconfiguration for your messaging services. Make sure that your MX mail records are set up properly to direct messages to the WatchGuard XCS.
- **Firewall** – If you have issues with your firewall, or if it is misconfigured, it may inadvertently block message access to and from the WatchGuard XCS. For example, SMTP port 25 access must be open between the Internet and the WatchGuard XCS, and between the WatchGuard XCS and internal servers to allow inbound and outbound message connections. TCP port 80 access is required for HTTP web communications between the WatchGuard XCS and external web servers.
- **Internal Messaging Systems** – You can experience problems where you receive incoming messages to the WatchGuard XCS, but the messages are not forwarded to the appropriate internal servers. Also, outgoing messages from the internal servers are not forwarded to the WatchGuard XCS for

delivery. In these scenarios, examine your internal messaging server to make sure it is working properly. Check communications between the two systems to make sure there are no network, DNS, or routing issues. Also check that your internal servers and web clients are configured to send outgoing messages and requests to the WatchGuard XCS.

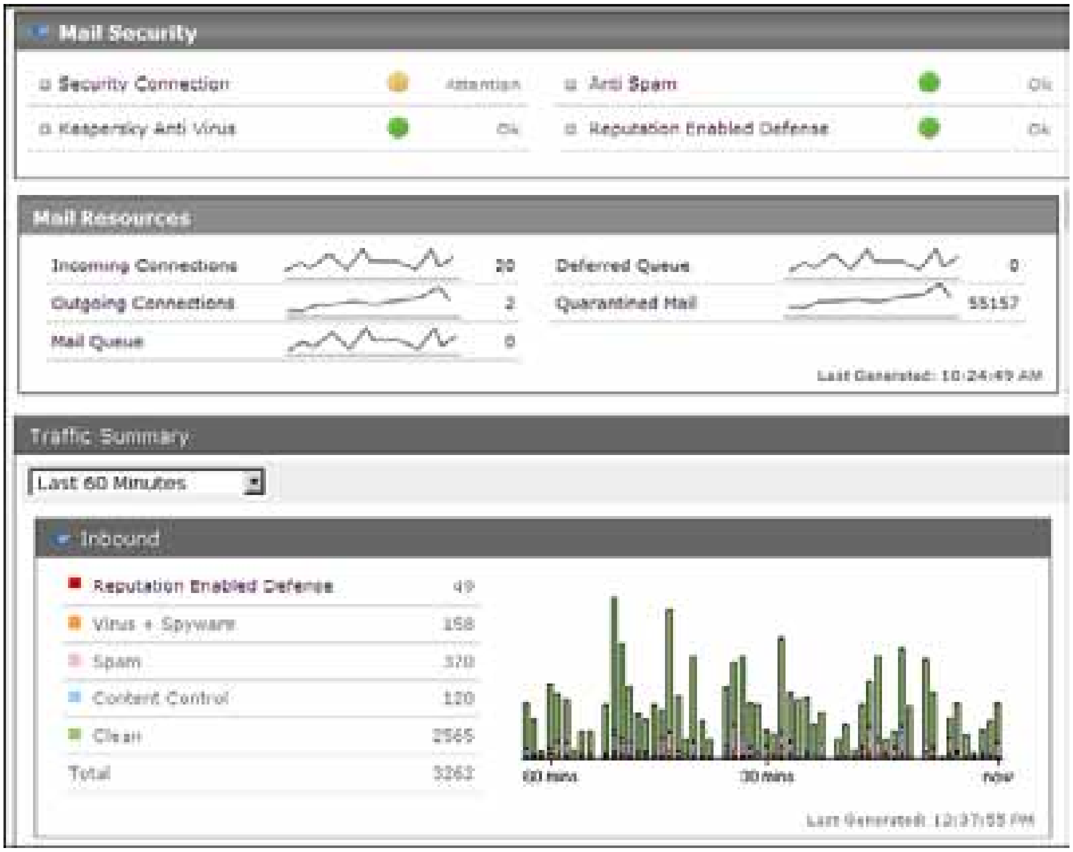
- **External Messaging and Web Servers** – If you have a large amount of messages or requests to a particular destination, and that server is currently down, the messages queue up in the deferred queue and delivery is retried after a period of time. You can view the log files to see the relevant messages that can indicate why you cannot connect to that particular server. The server could be down, too busy, or not currently accepting connections.

Troubleshooting Tools

These sections describe the built-in tools that you can use on the XCS device to help troubleshoot message and web request issues.

Monitor the Dashboard

The *Dashboard* provides a summary view that allows you to examine critical statistics for email and web traffic all on one page. When you check email and web activity, examine these items:



Mail Security

□ Security Connection	●	Attention	□ Anti Spam	●	Ok
□ Kaspersky Anti Virus	●	Ok	□ Reputation Enabled Defense	●	Ok

Mail Resources

Incoming Connections	20	Deferred Queue	0
Outgoing Connections	2	Quarantined Mail	55157
Mail Queue	0		

Last Generated: 10:24:49 AM

Traffic Summary

Last 60 Minutes

Inbound

🟥 Reputation Enabled Defense	49
🟧 Virus + Spyware	158
■ Spam	370
🟦 Content Control	120
🟩 Clean	2565
Total	3263

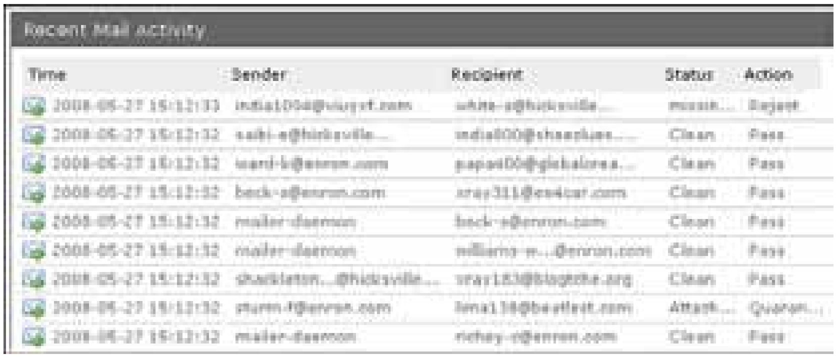
Last Generated: 12:37:55 PM

Check the **Mail Security** section to verify the status of your mail security services.

Check the **Mail Resources** section to view the number of messages in the *Mail Queue* and *Deferred* queue. This is a quick indicator of how your email messages are processing.

Make sure that the queues are not building up too high. This can indicate a message delivery issue. Also, check the number of incoming and outgoing connections, because you can experience system processing latency when a large number of concurrent connections are active.

In the *Recent Mail Activity* and *Recent Web Activity* portions of the *Dashboard*, check the timestamps of your most recent incoming and outgoing messages or web requests. If no messages or requests are processed in a specific period of time, this indicates that the inbound, outbound, or both directions are not working.

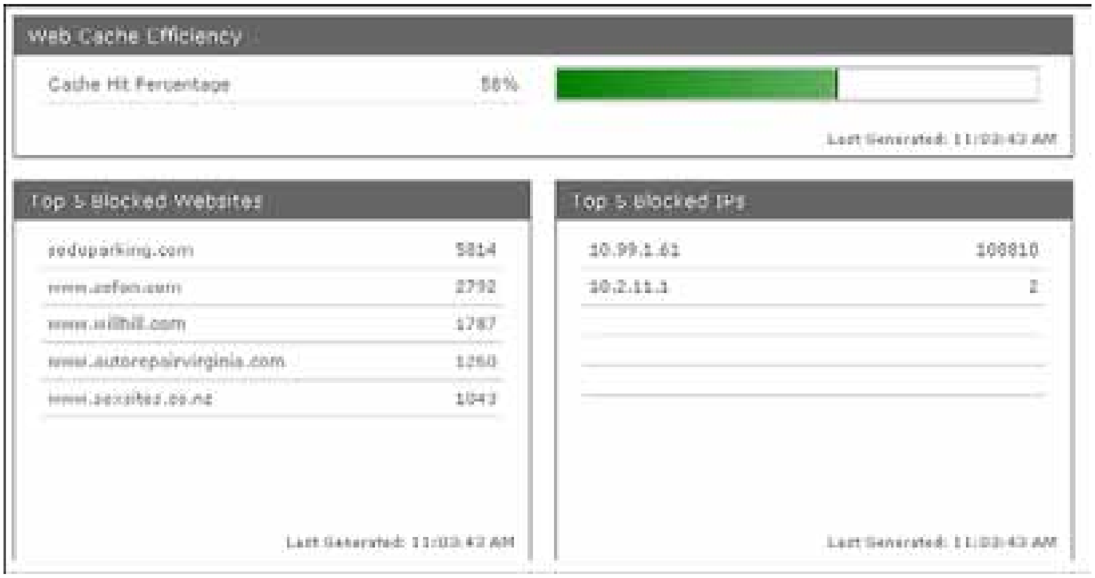


Recent Mail activity

Time	Sender	Recipient	Status	Action
2008-05-27 15:12:33	india1004@viaysrf.com	white-s@hicksville...	missin...	Reject
2008-05-27 15:12:32	saibi-e@hicksville...	india800@shaadiuas...	Clean	Pass
2008-05-27 15:12:32	ward-k@enron.com	papad00@globalarea...	Clean	Pass
2008-05-27 15:12:32	beck-s@enron.com	xray311@es4car.com	Clean	Pass
2008-05-27 15:12:32	mailer-daemon	beck-s@enron.com	Clean	Pass
2008-05-27 15:12:32	mailer-daemon	williams-w...@enron.com	Clean	Pass
2008-05-27 15:12:32	shackleton...@hicksville...	xray183@blogthe.org	Clean	Pass
2008-05-27 15:12:32	sturm-f@enron.com	lima138@beatlest.com	Attach...	Quaran...
2008-05-27 15:12:32	mailer-daemon	richey-c@enron.com	Clean	Pass

Check the mail and web traffic summaries regularly, because you may notice messaging system latency if you receive a lot of viruses, spam, or message rejects.

In the *Web Summary*, examine the web cache efficiency to make sure it is not at a low level compared to your typical cache efficiency baseline. Also, check the number of web connections, because you may experience system processing latency when a large number of connections are active.



Web Cache Efficiency

Cache Hit Percentage	58%

Last Generated: 11:03:43 AM

Top 5 Blocked Websites

sedoparking.com	5814
www.zofon.com	2792
www.willhill.com	1787
www.autorepairvirginia.com	1260
www.sexsites.co.nz	1043

Last Generated: 11:03:43 AM

Top 5 Blocked IPs

10.99.1.61	108810
10.2.11.1	2

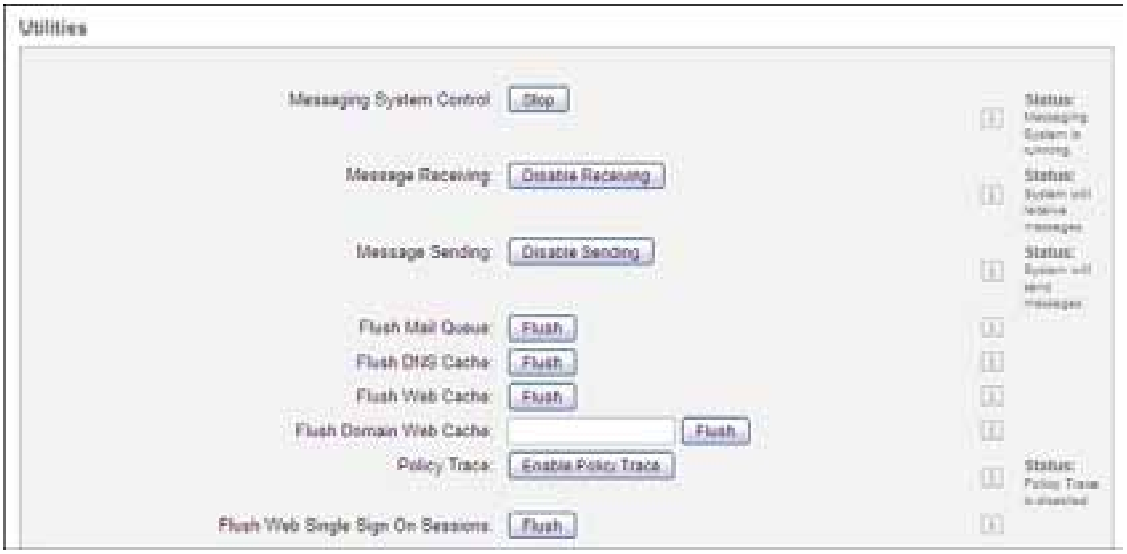
Last Generated: 11:03:43 AM

Network Utilities

Select **Activity > Status > Utilities** to access diagnostic tools that help you troubleshoot networking problems and connectivity issues with other messaging servers. Examples of messaging tools include Hostname Lookups, SMTP Probe, Ping, and Traceroute.

Utilities

From the *Utilities* section, you can control these system services:



Utilities

Messaging System Control: Stop — Status: Messaging System is running.

Message Receiving: Disable Receiving — Status: System will receive messages

Message Sending: Disable Sending — Status: System will send messages

Flush Mail Queue: Flush

Flush DNS Cache: Flush

Flush Web Cache: Flush

Flush Domain Web Cache: Flush

Policy Trace: Enable Policy Trace — Status: Policy Trace is disabled

Flush Web Single Sign On Sessions: Flush

Flush Mail Queue

Use the *Flush Mail Queue* option to flush and reprocess all queued email. You must only use this utility if you have a high amount of deferred mail that you need to deliver. This process can take a very long time in environments with a high amount of deferred mail.

If the deferred mail queue continues to grow, there are other problems that prevent the delivery of mail, and you should not click **Flush** again.

> ***Note*** *You must only click this button once because it reprocesses all queued mail.*

Flush DNS Cache

Click the **Flush** button to remote all entries from the current DNS cache. Use this option to clear the entries in the DNS cache if you experience issues resolving host names because of cached DNS queries.

Flush Web Cache

Click the **Flush** button to manually purge the Web Proxy disk cache. You should purge the entire web cache if you have issues with specific web pages not updating with newer content, or issues connecting to specific web sites.

Flush Domain Web Cache

You can flush the cache for a specific domain in the Web Proxy disk cache. You must specify the URL exactly how it is accessed, for example, www.example.com, or news.example.com. Subdomains are not included and you must flush each domain separately. Type a domain in the text box, then click **Flush**.

Policy Trace

Click **Policy Trace** to enable more detailed logging of policy resolution in the message logs.
The log entry contains information similar to this output:

```
policy_recipient=<testuser@example.com>,
policy_user=<testuser@example.com> (remote=F),
domain_policy=<2:Antispam enabled>, group_policy=<0:>,
group_name=<>, user_policy=<4:OCF enabled> default_policy=<1:Default>
```

Flush Web Single Sign On Sessions

Use this utility to flush all Web Proxy authenticated single sign-on sessions for both Proxy and Portal IP address-based authenticated users. After you flush the sessions, current Web Proxy users must authenticate to the Web Proxy again before they are allowed to browse web sites.

Hostname Lookup

Use the *Hostname Lookup* utility to perform DNS host lookups and make sure that hostnames are properly resolved by the DNS server.

To perform a hostname lookup:

1. In the **Name** text box, type the FQDN (Fully Qualified Domain Name) of the host to lookup on the name server.

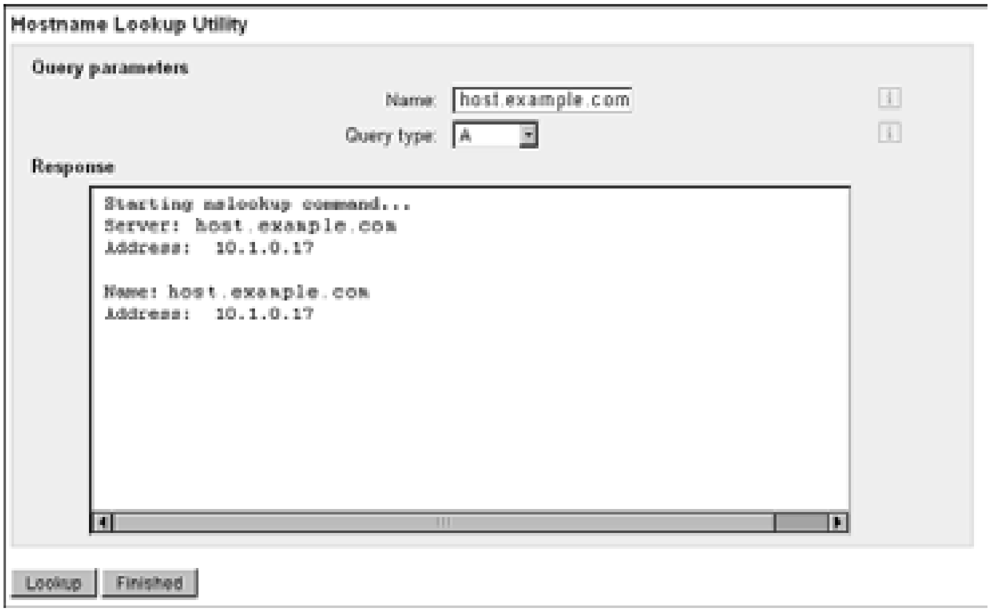
   For example, `host.example.com`.

2. From the **Query type** drop-down list, select the type of DNS record to lookup.

   For example, select **A** for a typical name host record or select **MX** for a mail server lookup.

3. Click **Lookup**.

   The name server displays the IP address for the host name. If “Unknown host” is displayed, then the host name is not listed in the DNS records.



Name: host.example.com

Query type: A

```
Starting nslookup command...
Server: host.example.com
Address:  10.1.0.17

Name: host.example.com
Address:  10.1.0.17
```

If the XCS device cannot contact the name server, select **Configuration > Network > Interfaces** and check your DNS configuration. To make sure you have network connectivity, use the ping and traceroute commands on the **Utilities** page to check if you have a connection to the network and to the DNS server.

The response displays the result of the SMTP diagnostic probe, and includes the response for each SMTP command:

```
Sending mail...
<<< 220 ESMTP Postfix (2.1.0)
HELO example.com
<<< 250 mail.example.com
MAIL FROM:user1@example.com
<<< 250 Ok

RCPT TO:user2@example.com

<<< 250 Ok

DATA

<<< 354 End data with <CR><LF>.<CR><LF>sending /tmp/smtpdata.

<<< 250 Ok: queued as F130F33EA6QUIT

<<< 221 Bye
```

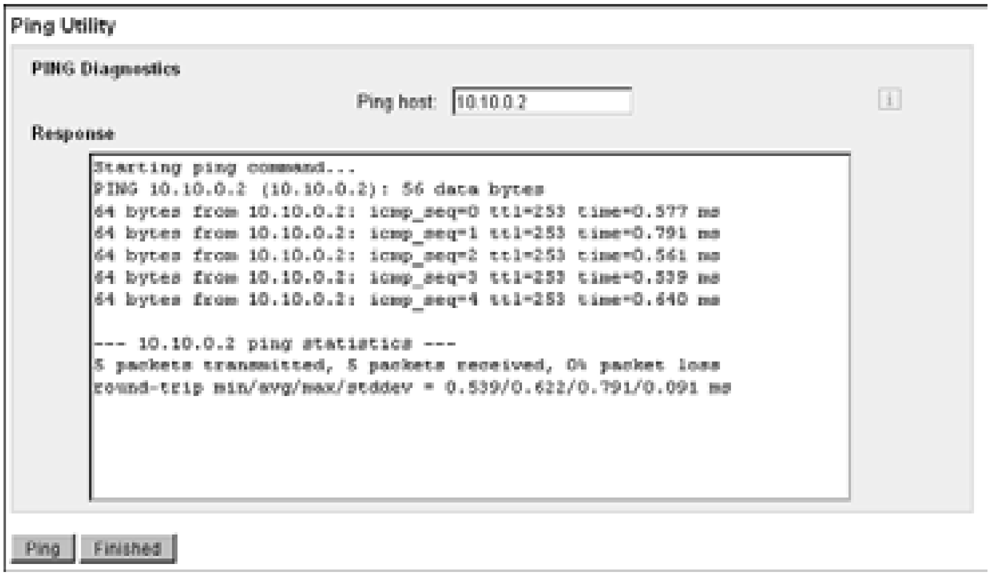
Ping Utility

The *ping* utility sends ICMP packets to a host and then listens for a return packet. Use this utility to ping hosts both on the internal and external networks from the WatchGuard XCS. Ping the firewall, DNS server, and external router, as well as the WatchGuard XCS from these locations to make sure you have connectivity. For more detailed information on routing connectivity between the two hosts, use the traceroute utility.

To test connectivity using ping:

1. In the **Ping host** text box, type the IP address or hostname of the host you want to ping.
2. Click **Ping**.

   The response displays the time for each successful ping. A “Request timed out” response indicates you cannot contact the specified host.



Ping host: 10.10.0.2

```
Starting ping command...
PING 10.10.0.2 (10.10.0.2): 56 data bytes
64 bytes from 10.10.0.2: icmp_seq=0 ttl=253 time=0.577 ms
64 bytes from 10.10.0.2: icmp_seq=1 ttl=253 time=0.791 ms
64 bytes from 10.10.0.2: icmp_seq=2 ttl=253 time=0.561 ms
64 bytes from 10.10.0.2: icmp_seq=3 ttl=253 time=0.539 ms
64 bytes from 10.10.0.2: icmp_seq=4 ttl=253 time=0.640 ms

--- 10.10.0.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.539/0.622/0.791/0.091 ms
```

Traceroute Utility

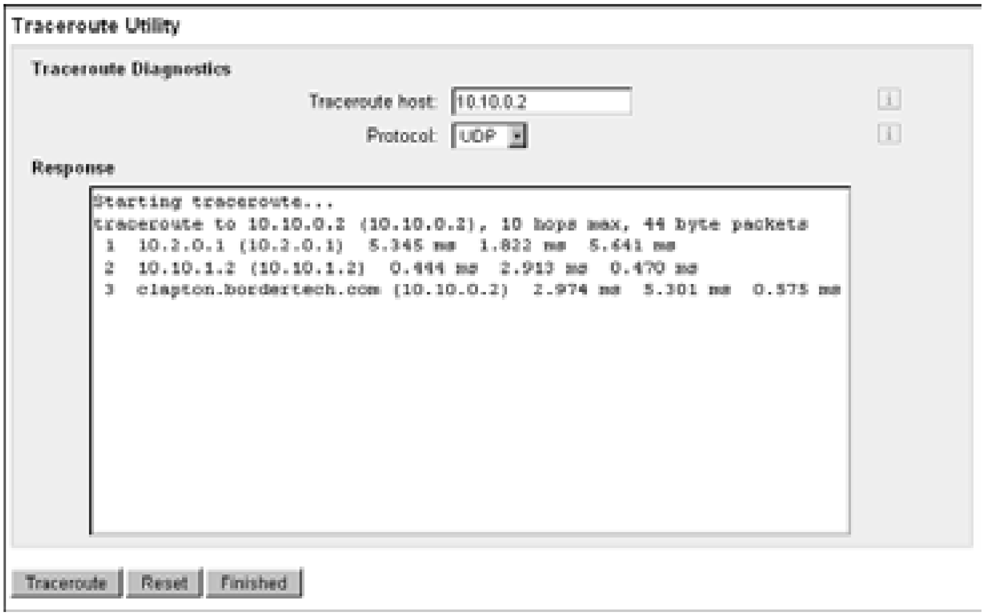
Use the *Traceroute* utility to see the routing steps between two hosts. If you lose connectivity somewhere between the XCS device and a receiving host, you can use traceroute to see where exactly the packet is dropped.

The traceroute utility displays each network hop as it passes through each router to the destination. If you experience routing issues, you can see in the trace output where exactly the communication fails.

To test connectivity using traceroute:

1. In the Traceroute host text box, type the IP address or host name of the system to test.
2. Click **Traceroute**.

   The response indicates the traceroute to the destination. A series of “*” characters indicates the connection is lost.



Traceroute Utility

Traceroute Diagnostics

Traceroute host: 10.10.0.2

Protocol: UDP

Response

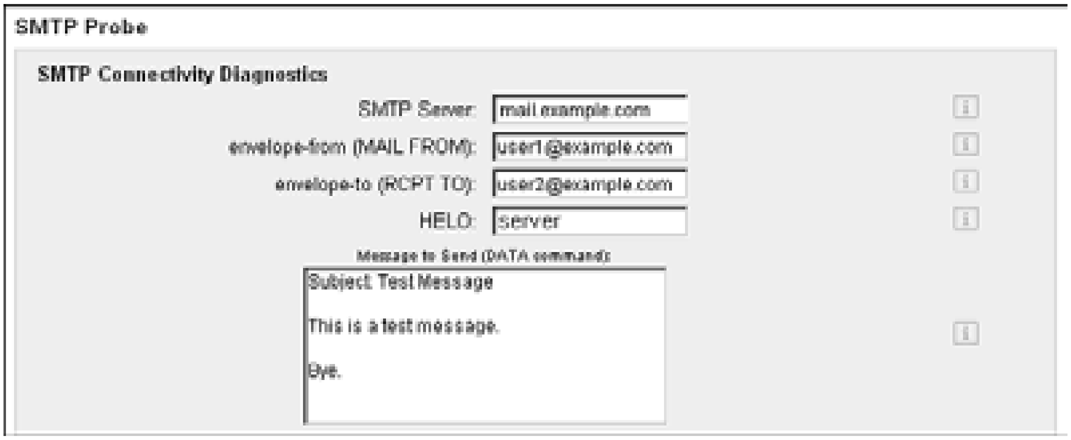
```
Starting traceroute...
traceroute to 10.10.0.2 (10.10.0.2), 10 hops max, 44 byte packets
 1  10.2.0.1 (10.2.0.1)  5.345 ms  1.822 ms  5.641 ms
 2  10.10.1.2 (10.10.1.2)  0.444 ms  2.913 ms  0.470 ms
 3  clapton.bordertech.com (10.10.0.2)  2.974 ms  5.301 ms  0.575 ms
```

SMTP Probe

Use the *SMTP (Simple Mail Transport Protocol) Probe* to test email connectivity with a remote SMTP server. This allows you to verify that the SMTP server responds to connection requests and returns a valid response.

To perform an SMTP probe:

1. In the **SMTP Server** text box, type the domain name or IP address of the destination SMTP server to test.



SMTP Probe

SMTP Connectivity Diagnostics

SMTP Server: mail.example.com

envelope-from (MAIL FROM): user1@example.com

envelope-to (RCPT TO): user2@example.com

HELO: server

Message to Send (DATA command):

Subject: Test Message

This is a test message.

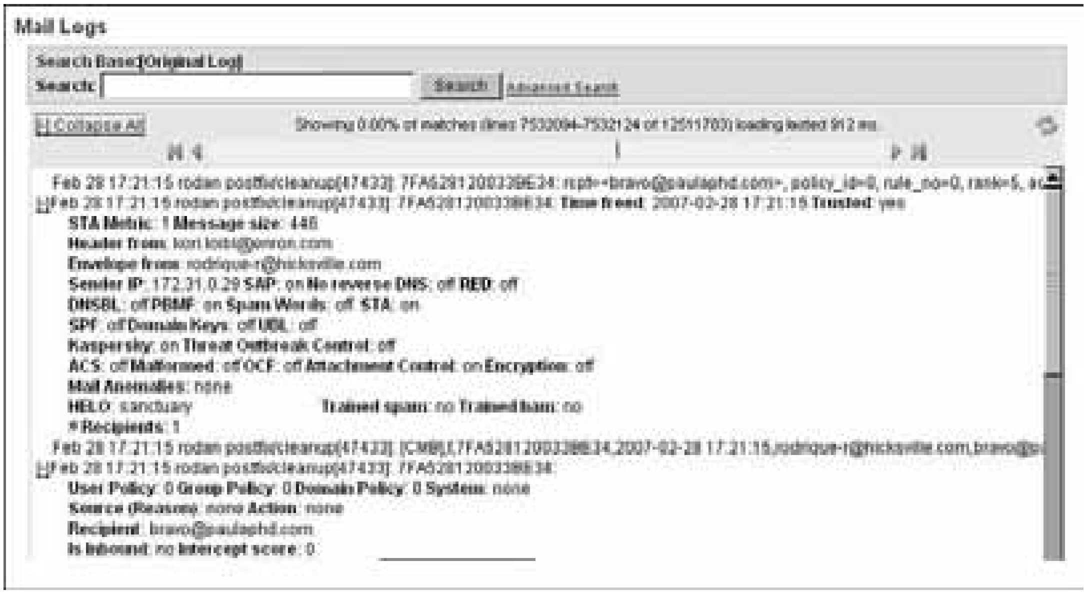
Bye.

2. In the **envelope-from (MAIL FROM)** text box, type the address to identify the sender of the email message.
3. In the **envelope-to (RCPT TO)** text box, type the address to identify the recipient of the email message.
4. In the **HELO** text box, type text that identifies the SMTP Client to the SMTP Server.
   You can enter any value here, but typically you specify the sending server’s domain name.

5. In the **Message to Send (DATA command)** text box, type the text to include in the test email message.
   You can enter an optional subject to make sure you do not send a message with a blank subject.
6. Click **Send Message**.

Examine Log Files

Select **Activity > Logs** to access logs files for each messaging protocol (Email and HTTP). These logs are the most important logs to monitor for message processing as they provide a detailed description of each message that passes through the XCS device.



```
Showing 0.00% of matches (lines 7532094-7532124 of 12511703) loading lasted 91.2 ms

  Feb 28 17:21:15 rodan postfix/cleanup[47433]: 7FA528120033BE34: rcpt=<bravo@paulaphd.com>, policy_id=0, rule_no=0, rank=5, ac
[-]Feb 28 17:21:15 rodan postfix/cleanup[47433]: 7FA528120033BE34: Time fixed: 2007-02-28 17:21:15 Trusted: yes
     STA Metric: 1 Message size: 446
     Header from: lori.lotti@enron.com
     Envelope from: rodrique-r@hicksville.com
     Sender IP: 172.31.0.29 SAP: on No reverse DNS: off RED: off
     DNSBL: off PBMF: on Spam Words: off STA: on
     SPF: off Domain Keys: off UBL: off
     Kaspersky: on Threat Outbreak Control: off
     ACS: off Malformed: off OCF: off Attachment Control: on Encryption: off
     Mail Anomalies: none
     HELO: sanctuary                    Trained spam: no Trained ham: no
     # Recipients: 1
  Feb 28 17:21:15 rodan postfix/cleanup[47433]: [CMB],7FA528120033BE34,2007-02-28 17:21:15,rodrique-r@hicksville.com,bravo@pa
[-]Feb 28 17:21:15 rodan postfix/cleanup[47433]: 7FA528120033BE34:
     User Policy: 0 Group Policy: 0 Domain Policy: 0 System: none
     Source (Reason): none Action: none
     Recipient: bravo@paulaphd.com
     Is Inbound: no Intercept score: 0
```

The start of a single message log entry begins with a “connect” message, and ends with the “disconnect” message. To make sure that you are looking at the entries for a specific message, check the Request ID (for web) or Message ID (for mail, for example, 7FA528120033BE34) for each log entry.

Click **[+]** or **[-]** to expand or collapse the log details for the specific Message or Request ID.

> **Note** *When there is more than one recipient for a message, only the first recipient is included in the log for the overall message summary.*

Troubleshoot Connection Issues

In many cases, a connection is blocked by the XCS device before the sending mail server transfers any messages. These features can trigger a connection-level reject:

- Reputation Enabled Defense
- DNS Block Lists
- Specific Access Patterns
- Pattern Filters
- Threat Prevention
- URL Block Lists

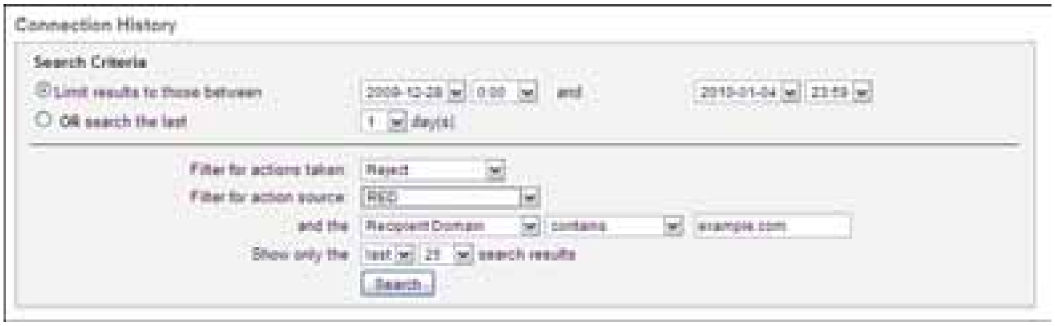
- Very Malformed messages
- Trusted/Blocked Senders Lists

To view a history of connections to the WatchGuard XCS:

1. Select **Activity > History > Connection History**.
2. Set the **Search Criteria** to limit the search to a specific range of dates or number of days.

   You can filter search results based on the actions taken on the connection and the action source, for example, a connection refused because of a low reputation by the Reputation Enabled Defense service.

   See *Connection History* for more information on searching the connection history database.



Connection History

Search Criteria

● Limit results to those between 2009-12-28 0:00 and 2010-01-04 23:59

○ OR search the last 1 day(s)

Filter for actions taken: Reject

Filter for action source: RED

and the: Recipient Domain contains example.com

Show only the: last 25 search results

Troubleshoot Content Issues

If a message is successfully delivered to the WatchGuard XCS, it undergoes security processing before it is delivered to its final destination. Many of the security tools used by the XCS device, for example, Intercept Anti-Spam, Content Filtering, Anti-Virus scanning, and Attachment Control, can reject, discard, or quarantine the message before it is delivered to the recipient. These tools can be misconfigured which allows legitimate messages and requests to be incorrectly rejected or quarantined. If specific messages are blocked when they should be allowed, check these items:

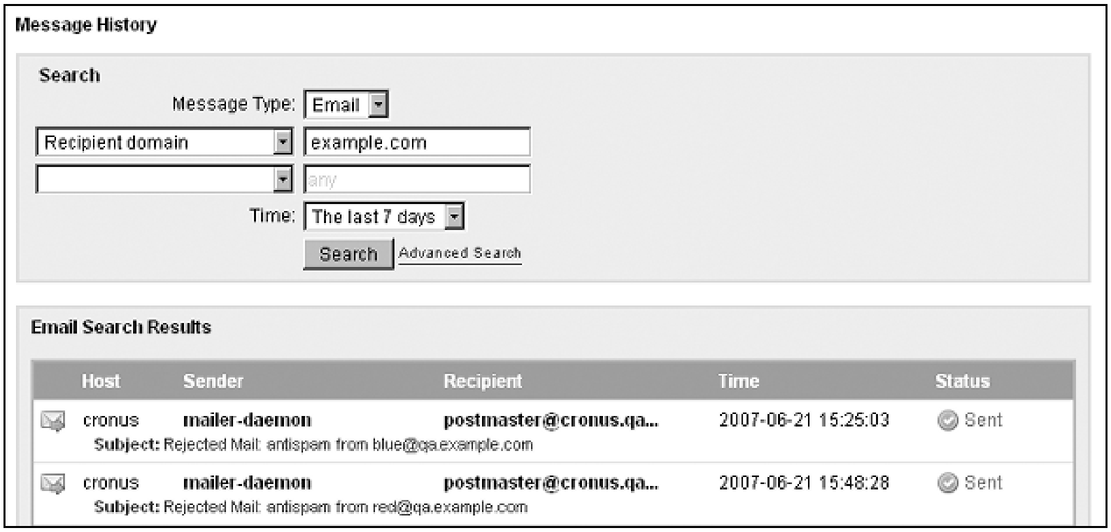
- Is there a Specific Access Pattern, Pattern Filter, or Content rule that applies to the message?
- Is the attachment type or content filtered by Attachment Control or Content Scanning?
- Do any of the Intercept Anti-Spam features block the message?
- Do words from the Objectionable Content Filter (OCF) or Spam Dictionaries appear in the message?
- Is the message or its attachments over the maximum size limit?
- Does the user belong to a policy that blocks the message?

Message History

Every email message and web request that passes through the WatchGuard XCS generates a database entry that records information about how it was processed, filtered, and delivered. To see how the message was processed, you can check the message history to see the disposition of the message. Use this information to find out which security process blocks the message, and then check the configuration and rules to make sure that they are set properly.

To view the Message History:

1. Select **Activity > History > Message History**.
2. Examine the *Status* column for full information on how a message was processed and its final disposition.



Message History

Search

Message Type: Email

Recipient domain: example.com

any

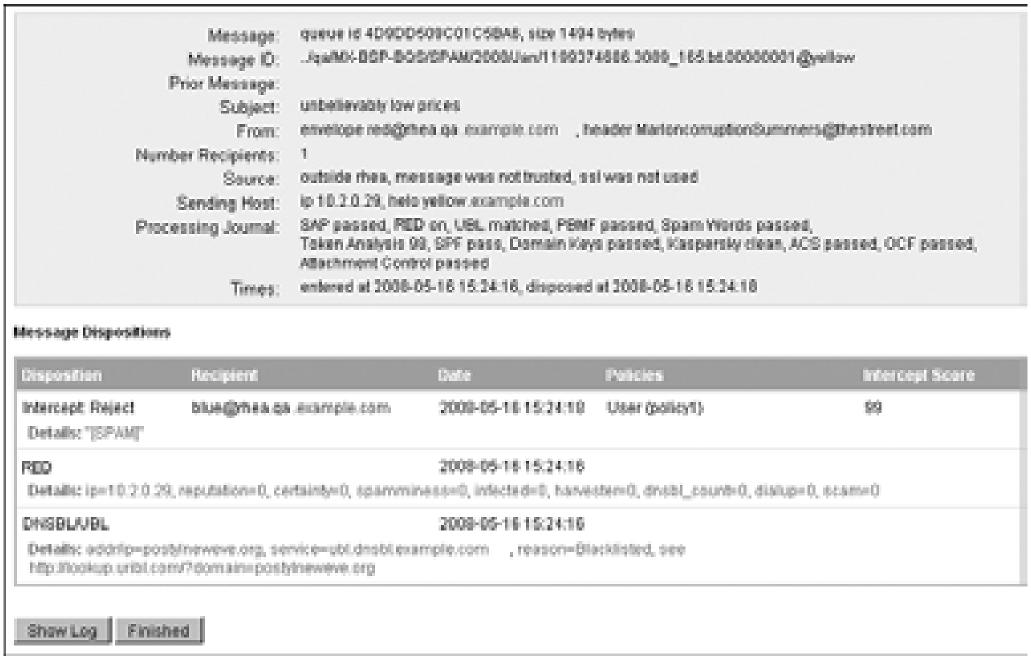
Time: The last 7 days

Email Search Results

Host	Sender	Recipient	Time	Status
cronus Subject: Rejected Mail: antispam from blue@qa.example.com	mailer-daemon	postmaster@cronus.qa...	2007-06-21 15:25:03	Sent
cronus Subject: Rejected Mail: antispam from red@qa.example.com	mailer-daemon	postmaster@cronus.qa...	2007-06-21 15:48:28	Sent

3. Click the **Message ID** to view the processing details of a message.

   Dispositions and the final Intercept score, if any, are listed below the details table in the *Message Disposition* section.



Message: queue id 4D9DD509C01C5BA6, size 1494 bytes
Message ID: ../qa/MX-BSP-BGS/SPAM/2008/Jan/1199374686.3089_165.txt.00000001@yellow
Prior Message:
Subject: unbelievably low prices
From: envelope red@rhea.qa.example.com , header MarlonCorruptionSummers@thestreet.com
Number Recipients: 1
Source: outside rhea, message was not trusted, ssl was not used
Sending Host: ip 10.2.0.29, helo yellow.example.com
Processing Journal: SAP passed, RED on, UBL matched, PBMF passed, Spam Words passed, Token Analysis 99, SPF pass, Domain Keys passed, Kaspersky clean, ACS passed, OCF passed, Attachment Control passed
Times: entered at 2008-05-16 15:24:16, disposed at 2008-05-16 15:24:18

Message Dispositions

Disposition	Recipient	Date	Policies	Intercept Score
Intercept: Reject Details: "[SPAM]"	blue@rhea.qa.example.com	2008-05-16 15:24:18	User (policy1)	99
RED Details: ip=10.2.0.29, reputation=0, certainty=0, spamminess=0, infected=0, harvester=0, dnsbl_count=0, dialup=0, scam=0		2008-05-16 15:24:16		
DNSBL/UBL Details: addr/ip=postlyneweve.org, service=ubl.dnsbl.example.com , reason=Blacklisted, see http://lookup.uribl.com/?domain=postlyneweve.org		2008-05-16 15:24:16		